MCCAULLEY LAW GROUP LLC
JOSHUA V. VAN HOVEN (CSB No. 262815)
E-Mail: josh@mccaulleylawgroup.com
3001 Bishop Dr., Suite 300
San Ramon, California 94583
Telephone: 925.302.5941

RICHARD T. MCCAULLEY (*pro hac vice*)
E-Mail: richard@mccaulleylawgroup.com
180 N. Wabash Avenue, Suite 601
Chicago, Illinois 60601
Telephone: 312.330.8105

Attorneys for Plaintiff and Counter-Defendant,
SURGICAL INSTRUMENT SERVICE COMPANY, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SURGICAL INSTRUMENT SERVICE COMPANY, INC. *Plaintiff/Counter-Defendant,* v. INTUITIVE SURGICAL, INC. *Defendant/Counterclaimant.*	CASE NO. 3:21-CV-03496-AMO Honorable Araceli Martínez-Olguín **PLAINTIFF SIS's MOTION IN LIMINE #4**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

RELIEF REQUESTED

Plaintiff Surgical Instrument Service Company Inc. ("SIS") respectfully moves in limine to limit the direct testimony of Defendant Intuitive Surgical, Inc.'s ("Intuitive") expert witness, Paul D. Martin, Ph.D., to the content of his Rule 26(a)(2)(B) report. To the extent Intuitive seeks to introduce at trial any opinion testimony[1] and argument, or question Dr. Martin about reverse engineering the technology necessary to reset X/Xi EndoWrists, including whether or not SIS could have broken the encryption on X/Xi EndoWrists, such evidence should be excluded because it is outside the content of Dr. Martin's expert report. SIS also seeks the exclusion of all undisclosed opinion evidence and any lines of questioning about the feasibility, timing, resources needed, and effort required to defeat the encryption on the RFID chip so as to access and reset the X/Xi EndoWrist usage counter. These matters are likewise beyond the scope of any opinion Dr. Martin offered in his expert report.

Any opinion testimony and argument on these issues, proffered now for the first time by Intuitive, should be recognized for what it really is: a belated attempt to generate a rebuttal case that Intuitive deliberately chose not to proffer through Dr. Martin, its own expert. Accordingly, such opinion testimony and argument should be excluded because Intuitive failed to comply with the disclosure requirements of the Federal Rules of Civil Procedure and the limitations on lay witness opinion testimony set by the Rules of Civil Procedure and Rules of Evidence.

BACKGROUND

In his opening report, SIS's expert Kurt Humphrey[2] opined, *inter alia*, that:

> 14. The encryption on X and Xi EndoWrists requires substantially more computing resources to reverse engineer than the encryption of Si EndoWrists. Although the encryption techniques utilized by Intuitive for the use counters of the X and Xi EndoWrists can, and in fact have been, reverse engineered with adequate computing power and resources, as compared to the encryption used for the use counter of the Si EndoWrists, the Xi encryption requires substantially more time and resources to reverse engineer.

[1] For purposes of this motion, "testimony" includes lay person and expert testimony presented at trial either live or through video recordings of deposition testimony.

[2] Mr. Humphrey is SIS's expert in reverse engineering, integrated circuits, and wireless communication systems including RFID systems.

> 15. Reverse engineering of the X and Xi EndoWrist encryption is simply a matter of computing power and financial resources. The time necessary to reverse engineer an X or Xi EndoWrist would be compressed with additional resources, and would have been possible within a similar time frame at least as early as 2019.

Van Hoven Exh. 1, Expert Report of Kurt Humphrey (December 2, 2022).[3] Intuitive's expert, Paul D. Martin, Ph.D., was asked to review and opine on Kurt Humphrey's expert report and the subjects covered therein. *See* Van Hoven Exh. 2 at ¶ 19, Expert Report of Paul D. Martin, Ph.D. (January 18, 2023). Dr. Martin, however, provided no opinions regarding whether the encryption techniques that Intuitive used for the use counters of the X/Xi EndoWrists can be, and in fact have been, reverse engineered with adequate computing power and resources. He also fails to proffer any opinions or analyses on the extent of the time and resources needed to reverse engineer the encryption used for X/Xi instruments. Dr. Martin makes only one comment in his report to rebut Mr. Humphrey's opinions: "Finally, it is my opinion that reverse engineering the X/Xi instruments involves a different process than reverse engineering the S/Si instruments, though Mr. Humphrey's analysis on the extent of the time and resources needed to reverse engineer the X/Xi instruments is speculative." *Id.* at ¶¶ 25, 74–78.

In his deposition, Dr. Martin confirmed that he had not conducted any analyses nor formulated any opinions regarding the feasibility, timing, resources needed, and effort required to reverse engineer the X/Xi EndoWrists encryption and reset the usage counter. For example, Dr. Martin refused to opine on or even consider X and Xi encryption. Van Hoven Exh. 3 197:15–19 ("Yeah, I haven't performed an analysis of what would be required to break the [Xi EndoWrist]."); Id. at 190:2–6 ("I don't have an opinion on" whether "the encryption employed by [the chip used in X/Xi EndoWrists] is particularly complicated compared with the sort of encryption you typically have worked with[.]"); *id.* at 187:5–11 ("So, I – I just haven't done

[3] Mr. Humphrey also opined that "Intuitive's reason for employing encrypted communication between the X/Xi robots and the EndoWrists was to prevent modification of the use counter. The electronics within the Intuitive X and Xi EndoWrists do not actively control the EndoWrist, and third parties have only attempted to access or reverse engineer the use counter, not any other functionality of Si or X/Xi EndoWrists. Preventing third parties from accessing the use counter was Intuitive's primary concern when it selected the encryption used with Xi EndoWrists, and to this day Intuitive encrypts the communication of use counter data but does not encrypt communication of safety-critical patient sensor data." Van Hoven Exh. 1 at ¶ 16.

that analysis" of how one "would . . .go about trying to circumvent the encryption on the use counter within [the chip used in the X/Xi.]"); *id.* at 188:3–189:7 ("I would need some time thinking about it"; "I haven't really thought about it"; "Yes, I would have to think about that"); *id.* at 198:12–14 ("So, it's a multi-step process, and I haven't performed even the first step yet is the problem."). Although Dr. Martin never performed any "legwork" and refused to discuss what "legwork" would be involved in examining X/Xi encryption, he similarly admits that solving encryption problems is a matter of "legwork." *Id.* at 187:5–189:7; 196:16–198:19.

Nevertheless, SIS suspects that Intuitive will attempt to introduce undisclosed opinion testimony and argument at trial based on Intuitive's vigorous efforts to reopen discovery. For example, Intuitive sought leave to pursue further document and deposition discovery from non-parties relating to "the progress, if any, that third-party companies have made in the past two years towards developing the technology necessary to reset EndoWrists that are compatible with the newer X/Xi model da Vinci surgical robots" Dkt. 243-1 at pp. 2, 12.

ARGUMENT

Legal Standards - Motions in Limine

"A motion in limine is a procedural mechanism to limit in advance testimony or evidence in a particular area." *United States v. Heller*, 551 F.3d 1108, 1111 (9th Cir. 2009). Motions in limine are vehicles by which a court may exclude inadmissible or prejudicial evidence before it is "actually offered." *See Luce v. United States*, 469 U.S. 38, 40 n.2 (1984). Motions in limine "avoid the futile attempt of unringing the bell when jurors have seen or heard inadmissible evidence, even when stricken from the record"; "streamline trials, by settling evidentiary disputes in advance and by minimizing side-bar conferences and other disruptions at trial"; and "permit more thorough briefing and argument on evidentiary issues than would be likely during trial." *Altair Instruments, Inc. v. Telebrands Corp.*, 2021 WL 5238787, at *1 (C.D. Cal. Feb. 18, 2021) (cleaned up). "[M]otions in limine must identify the evidence at issue and state with specificity why such evidence is inadmissible." *United States v. Lewis*, 493 F. Supp. 3d 858, 861 (C.D. Cal. 2020) (cleaned up) (citation omitted).

Admissibility of Opinion Evidence Requires Compliance With the Rules of Civil Procedure and Rules of Evidence

Parties must disclose the identity of any expert witness they may use at trial, along with a written report prepared and signed by the witness. Fed. R. Civ. P. 26(a)(2) (A), (B). "An expert report is to be a detailed and complete statement of the testimony of the expert on direct examination." *Atmel Corp. v. Information Storage Devices, Inc.*, 189 F.R.D. 410, 415 (N.D. Cal. 1999)(citations omitted). The parties "must make these disclosures at the times and in the sequence that the court orders." Fed. R. Civ. P. 26(a)(2)(D). A party must supplement its disclosures: (a) in a timely manner if it learns that the initial disclosures were incomplete or incorrect; or (b) as ordered by the court. Fed. R. Civ. P. 26(a)(2)(E), 26(e)(1). For an expert who provides a report, the "duty to supplement extends both to information included in the report and to information given during the expert's deposition." Fed. R. Civ. P. 26(e)(2). If a party fails to comply with the requirements of Rule 26(a) or (e), such party "is not allowed to use that information or witness to supply evidence on a motion, at a hearing, or at trial, unless the failure was substantially justified or is harmless." Fed. R. Civ. P. 37(c)(1); *Goodman v. Staples The Office Superstore, LLC*, 644 F.3d 817, 827 (9th Cir.2011); see also *Yeti by Molly, Ltd. v. Deckers Outdoor Corp.*, 259 F.3d 1101, 1106 (9th Cir. 2001) (explaining Rule 37(c)(1) "gives teeth" to the requirements of Rule 26); *see also Eisen v. Day*, 2024 WL 1244482, * 4 (N.D. Cal. March 21, 2024). "Overall, the purpose of Rule 26's provisions governing expert reports and depositions is to ensure that the opposing party can ascertain the expert's opinions and conclusions on pertinent subjects prior to trial, and avoid unfair surprise." *MJC America, Ltd. v. Gree Electric Appliances, Inc.,* 2015 WL 12747825, * 2 (C.D. Cal. April 27, 2015) (citations omitted).

"Under the normal operation of Rules 26 and 37 of the Federal Rules of Civil Procedure, an expert may not extend his or her direct testimony beyond the opinions and bases disclosed in the Rule 26(a)(2)(B) report and may not, on direct examination, cover new work done thereafter." *Atmel Corp.*, 189 F.R.D. at 411. "Most courts have concluded that '[e]xpert witnesses . . . are precluded from testifying at trial as to their opinions on subject matters upon

which they did not state opinions . . . at the time their depositions were taken.'". *MJC America,* 2015 WL 12747825, * 3 (citations omitted). "Excluding an expert's trial testimony where it pertains to subjects about which the expert claimed not to have an opinion during his deposition streamlines trial and prevents unfair surprise to the opposing party." *Id.* (citations omitted). Intuitive cannot seriously contend that Dr. Martin should be allowed, on direct examination, to offer new opinions beyond the scope of his report. To now permit Dr. Martin to testify on direct examination to matters deliberately ignored in his Rule 26(a)(2)(B) report and which he was not prepared to testify about at his deposition would simply encourage litigants to evade the expert-disclosure rules. *See Id.* at 416.

To the extent that Intuitive attempts at trial to offer lay opinion testimony about the feasibility, timing, resources needed, and effort required to reverse engineer the X/Xi EndoWrist encryption and reset the usage counter, such evidence should be excluded as failing to comply with Fed. R. Evid. 701. Under Federal Rule of Evidence 701, lay opinion testimony is permitted where the opinion is a) rationally based on the witness's perception, b) helpful to clearly understanding the witness's testimony or to determining a fact in issue, and c) **not based on scientific, technical, or other specialized knowledge within the scope of Rule 702**. *See Haro v. GGP-Tucson Mall LLC,* 2019 WL 369269, * 4–5 (D. Arizona January 30, 2019). Since opining about reverse engineering the X/Xi EndoWrist encryption in order to reset the usage counter would be based on scientific, technical, or other specialized knowledge within the scope of Rule 702, lay opinion testimony directed to that subject matter area would be impermissible. *See Sapiano v. Millennium Entertainment,* 2013 WL 12122467, * 4 (C.D. Cal. November 20, 2013). Intuitive's lay witnesses should be barred from offering testimony at trial beyond that which Rule 701 permits. *See Malkin v. Federal Insurance Company*, 2023 WL 6967458, * 16 (C.D. Cal. October 20, 2023).

Additionally, Intuitive should be precluded from offering any non-retained expert testimony from its employees at trial. Even though an expert report is not required under Rule 26(a)(2)(B), Intuitive was required to identify any non-retained expert under Rule 26(a)(2)(A), otherwise that witness would not be permitted to express expert opinions. Fed. R. Civ. P.

37(c)(1). Mere identification of a person is not sufficient to meet the requirements of Rule 26(a)(2)(A). Further, non-retained experts are required to disclose their actual and specific opinions under Rule 26(a)(2)(C). Without identification as an **expert** witness, accompanied by the required disclosures, SIS is not on fair notice and would be prejudiced if Intuitive was permitted to present undisclosed expert testimony from any of its employees. *See Monster Energy Company v. Integrated Supply Network, LLC*, 2018 WL 11504608 (C.D. Cal. August 23, 2018).

CONCLUSION

For the foregoing reasons, Plaintiff SIS respectfully requests that the Court grant this motion in limine #4, excluding Intuitive from presenting testimony, documentary evidence, and argument about reverse engineering the technology necessary to reset X/Xi EndoWrists, including whether or not SIS could have broken the encryption on X/Xi EndoWrists. Further, SIS respectfully requests that the Court exclude all undisclosed opinion evidence and any lines of questioning about the feasibility, timing, resources needed, and effort required to defeat the encryption on the RFID chip so as to access and reset the X/Xi EndoWrist usage counter.

Dated: October 28, 2024

McCAULLEY LAW GROUP LLC
By: */s/ Joshua Van Hoven*
JOSHUA V. VAN HOVEN

E-Mail: josh@mccaulleylawgroup.com
3001 Bishop Dr., Suite 300
San Ramon, California 94583
Telephone: 925.302.5941

RICHARD T. MCCAULLEY (*pro hac vice*)
E-Mail: richard@mccaulleylawgroup.com
180 N. Wabash Avenue, Suite 601
Chicago, Illinois 60601
Telephone: 312.330.8105

Attorneys for Plaintiff and Counter-Defendant,
SURGICAL INSTRUMENT SERVICE COMPANY, INC.

CERTIFICATE OF SERVICE

I hereby certify that on October 28, 2024, I caused a copy of the foregoing **PLAINTIFF SIS's MOTION IN LIMINE #4**, to be electronically to be served *via* electronic mail to counsel of record:

Crystal Lohmann Parker
Paul, Weiss, Rifkind, Wharton & Garrison LLP
1285 Avenue of the Americas
New York, NY 10019
212-373-3000
Email: cparker@paulweiss.com

Joshua Hill , Jr.
Paul, Weiss, Rifkind, Wharton & Garrison LLP
535 Mission Street, 24th Floor
San Francisco, CA 94105
(628) 432-5123
Email: jhill@paulweiss.com

Kenneth A. Gallo
Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street NW
Washington, DC 20006-104 7
202-223-7356
Fax: 202-204-7356
Email: kgallo@paulweiss.com

Paul David Brachman
Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K St., NW
Washington, DC 20006
202-223-7440
Email: pbrachman@paulweiss.com

William Michael
Paul, Weiss, Rifkind, Wharton and Garrison LLP
1285 Avenue of the Americas
New York, NY 10019
212-373-3000
Email: WMichael@paulweiss.com

Allen Ruby
Attorney at Law
15559 Union Ave. #138
Los Gatos, CA 95032
408-4 77-9690
Email: allen@allenruby.com

Andrew David Lazerow
Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956
202-662-5081
Email: alazerow@cov.com

Kathryn Elizabeth Cahoy
Covington & Burling LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, CA 94306
650-632-4700
Email: kcahoy@cov.com

Sonya Diane Winner
Covington & Burling LLP
Floor 54
415 Mission Street
San Francisco, CA 94105-2533
(415) 591-6000
Email: swinner@cov.com

Dated: October 28, 2024

By: */s/ Joshua Van Hoven*
JOSHUA V. VAN HOVEN

MCCAULLEY LAW GROUP LLC
JOSHUA V. VAN HOVEN (CSB No. 262815)
E-Mail: josh@mccaulleylawgroup.com
3001 Bishop Dr., Suite 300
San Ramon, California 94583
Telephone: 925.302.5941

RICHARD T. MCCAULLEY (*pro hac vice*)
E-Mail: richard@mccaulleylawgroup.com
180 N. Wabash Avenue, Suite 601
Chicago, Illinois 60601
Telephone: 312.330.8105

Attorneys for Plaintiff and Counter-Defendant,
SURGICAL INSTRUMENT SERVICE COMPANY, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SURGICAL INSTRUMENT SERVICE COMPANY, INC. *Plaintiff/Counter-Defendant,* v. INTUITIVE SURGICAL, INC. *Defendant/Counterclaimant.*	CASE NO. 3:21-CV-03496-AMO Honorable Araceli Martínez-Olguín **DECLARATION OF JOSHUA VAN HOVEN IN SUPPORT OF PLAINTIFF SIS's MOTION IN LIMINE #4**

I, JOSHUA VAN HOVEN, declare as follows:

I am an attorney at the law firm of MCCAULLEY LAW GROUP LLC, attorneys for Plaintiff SURGICAL INSTRUMENT SERVICE COMPANY, INC. ("SIS") in this matter. I have personal knowledge of the matters set forth herein, unless otherwise noted.

1. Attached as Exhibit 1 is a true and correct copy of a redacted version of the Expert Report of Kurt Humphrey, an SIS expert in this case, which is dated December 2, 2022 - the portions that are attached hereto were previously filed on the public docket at Dkt. 229-14.
2. Attached as Exhibit 2 is a true and correct copy of a redacted version of the Expert Report of Paul D. Martin, PhD., an Intuitive expert in this case, which is dated January 18, 2023 - the portions that are attached hereto were previously filed on the public docket at Dkt. 229-10.
3. Attached as Exhibit 3 is a true and correct copy of excerpts of the Deposition of Paul D. Martin, PhD., which was taken on March 16, 2023, and previously filed on the public docket at Dkt. 228-32.

I declare under the penalty of perjury under the laws of the United States that the foregoing is true and correct.

Dated: October 28, 2024

McCAULLEY LAW GROUP LLC
By: */s/ Joshua Van Hoven*
JOSHUA V. VAN HOVEN

E-Mail: josh@mccaulleylawgroup.com
3001 Bishop Dr., Suite 300
San Ramon, California 94583
Telephone: 925.302.5941

RICHARD T. MCCAULLEY (*pro hac vice*)
E-Mail: richard@mccaulleylawgroup.com
180 N. Wabash Avenue, Suite 601
Chicago, Illinois 60601
Telephone: 312.330.8105

Attorneys for Plaintiff and Counter-Defendant,
SURGICAL INSTRUMENT SERVICE COMPANY, INC.

CERTIFICATE OF SERVICE

I hereby certify that on October 28, 2024, I caused a copy of the foregoing **DECLARATION OF JOSHUA VAN HOVEN IN SUPPORT OF PLAINTIFF SIS's MOTION IN LIMINE #4**, to be electronically to be served *via* electronic mail to counsel of record:

Crystal Lohmann Parker
Paul, Weiss, Rifkind, Wharton & Garrison LLP
1285 Avenue of the Americas
New York, NY 10019
212-373-3000
Email: cparker@paulweiss.com

Joshua Hill , Jr.
Paul, Weiss, Rifkind, Wharton & Garrison LLP
535 Mission Street, 24th Floor
San Francisco, CA 94105
(628) 432-5123
Email: jhill@paulweiss.com

Kenneth A. Gallo
Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street NW
Washington, DC 20006-104 7
202-223-7356
Fax: 202-204-7356
Email: kgallo@paulweiss.com

Paul David Brachman
Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K St., NW
Washington, DC 20006
202-223-7440
Email: pbrachman@paulweiss.com

William Michael
Paul, Weiss, Rifkind, Wharton and Garrison LLP
1285 Avenue of the Americas
New York, NY 10019
212-373-3000
Email: WMichael@paulweiss.com

Allen Ruby
Attorney at Law
15559 Union Ave. #138
Los Gatos, CA 95032
408-4 77-9690
Email: allen@allenruby.com

Andrew David Lazerow
Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956
202-662-5081
Email: alazerow@cov.com

Kathryn Elizabeth Cahoy
Covington & Burling LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, CA 94306
650-632-4700
Email: kcahoy@cov.com

Sonya Diane Winner
Covington & Burling LLP
Floor 54
415 Mission Street
San Francisco, CA 94105-2533
(415) 591-6000
Email: swinner@cov.com

Dated: October 28, 2024

By: */s/ Joshua Van Hoven*
JOSHUA V. VAN HOVEN

Exhibit 1

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SURGICAL INSTRUMENT SERVICE COMPANY, INC.,

Plaintiff/Counter-Defendant,

v.

INTUITIVE SURGICAL, INC.,

Defendant/Counterclaimant.

Case No. 3:21-cv-03496-VC

Honorable Vince Chhabria

EXPERT REPORT OF KURT HUMPHREY

Complaint Filed: May 10, 2021

Highly Confidential – Subject to Protective Order

TABLE OF CONTENTS

I. QUALIFICATIONS

1. I currently work as Managing Director and Principal Technologist at IP Enginuity LLC. I have held that position for the past 17 years.

2. I hold B.S. and M.S. degrees in Ceramic Engineering from the University of Missouri-Rolla and worked primarily as a Process Development Engineer and Process Integration Manager during my 20+ year history in integrated circuit (IC) device and smart sensor processing. My professional experience in industry included responsibilities for complementary metal oxide semiconductor (CMOS) process development for DRAM, SRAM, EEPROM and SONOS flash and embedded non-volatile (NV) memories at AT&T Technologies, Philips Research Laboratories in Eindhoven, NL, and United Technologies Microelectronics Center. While at Philips, I collaborated with engineers at Siemens (DE), IBM (US), Intel (US), Motorola (US), Texas Instruments (US) and SEMATECH (US) on next-generation memory technology through formal technology transfer agreements with Philips (NL).

3. I am an expert in reverse engineering (RE) industrial and consumer microelectronic devices, components and systems including RFID products such as smart EMV smartcards and other proximity integrated circuit cards (PICCs). Over the course of my career, I have reverse engineered a large number and wide variety of semiconductor devices including microprocessors and non-volatile memories such as EEPROMs and Flash products for OEMs such as Apple, Alcatel-Lucent (Nokia) and others.

4. I have been engaged by multiple clients to extract or "dump" contents of specific EEPROMs and flash memories used in contactless RFID smart cards such as Visa payWave, Gemalto and other contactless EMV cards. The primary objective was to analyze the code or firmware with respect to patent enforcement/infringement matters.

5. I have general familiarity with encryption and security used in RFID communications, including encryption via stream ciphers and mutual authentication protocols.

6. A copy of my current *Curriculum Vitae* is attached to this report at Attachment 1.

II. PRIOR TESTIMONY AND PUBLICATIONS

7. I have been deposed as a technical expert nine times and provided expert trial testimony the following cases:

a. I was engaged as an expert by Rebotix Repair LLC regarding reverse engineering and resetting of the use counter for Xi EndoWrists.[1] I was deposed in that matter.

b. I was engaged as an expert by Hewlett Packard in an International Trade Commission (ITC) patent infringement case in 2006/2007 against Acer.[2] I provided reverse engineering and technical product testing services, prepared an expert report based on my empirical findings and was subsequently deposed.

c. I was engaged as an expert by Clutch City Sports and Entertainment, L.P. in a matter against iLight Technologies, Inc.[3] I performed failure analyses on sample products, prepared an expert report, was deposed, and testified before a jury.

d. I was engaged as an expert by General Access Solutions, LTD where I submitted an expert report and was deposed.[4].

[1] *Rebotix Repair LLC v. Intuitive Surgical, Inc.*, Case No. 8:20-cv-02274 (M.D. Fla)
[2] Personal Computers and Digital Display Devices, ITC Inv. No. 337-TA-606 (*Hewlett Packard v. Acer, Inc. et al.*)
[3] *Clutch City Sports & Entertainment, L.P. v. iLight Technologies, Inc. et al.*, Cause No. 2009-76645 (157th Dist. Ct., Harris County, TX Nov. 2009)
[4] *Sprint Spectrum L.P. v. General Access Solutions, LTD*, Case No. IPR2017-001889 (PTAB 2017)

e. I was engaged as an expert by Proxense LLC in a patent infringement case involving Bluetooth Low Energy technology where I submitted an expert report regarding claim construction and was also deposed.[5]

f. I was engaged by Neogen Corp. in a case where I provided an expert report, trial for which is scheduled for June 2022.[6]

g. I was engaged by Ocean Semiconductor LLC in a case where I provided an expert declaration and was deposed. [7]

h. I was engaged by Ocean Semiconductor LLC in a case where I provided an expert declaration and was deposed. [8]

i. I was engaged by Ocean Semiconductor LLC in a case where I provided an expert declaration and was deposed. [9]

j. I was engaged by Ocean Semiconductor LLC in a case where I provided an expert declaration and was deposed. [10]

k. I was engaged by Ocean Semiconductor LLC in a case where I provided an expert declaration and was deposed. [11]

[5] *Proxense LLC v. Target Corporation*, Case No.6:20-cv-879 (W.D. Tex.)
[6] *Neogen Corp. v. Innovative Reproductive Technology LLC*, Case No. 4:19-cv-00330-RGE-CFB (S.D. IOWA)
[7] *Western Digital Technologies, Inc. v. Ocean Semiconductor LLC*, Case No. IPR Case IPR2021-00929 (PTAB 2021)
[8] *Applied Materials, Inc. v. Ocean Semiconductor LLC*, Case No. IPR2021-01340 (PTAB 2021)
[9] *Applied Materials, Inc. v. Ocean Semiconductor LLC*, Case No. IPR2021-01342 (PTAB 2021)
[10] *Applied Materials, Inc. v. Ocean Semiconductor LLC*, Case No. IPR2021-01344 (PTAB 2021)
[11] *ST Microelectronics, Inc. v. Ocean Semiconductor LLC*, Case No. IPR2021-01349 (PTAB 2021)

8. A list of all publications I have authored or co-authored during the past ten years is included in my *Curriculum Vitae*, attached to this report at Attachment 1.

9. I am listed as an inventor or co-inventor on the patents listed in Attachment 1.

III. ENGAGEMENT AND COMPENSATION

10. I am submitting this report at the request of Haley Guiliano LLP, counsel for Surgical Instrument Service Company, Inc. ("SIS"), the named plaintiff in the lawsuit captioned on this report's first page. This report sets forth opinions I have formed about which I may testify if called as a witness at the trial of this lawsuit.

11. I am an independent expert with extensive experience in reverse engineering, integrated circuits, and wireless communication systems including RFID systems. I have been asked to provide opinions about the encryption utilized on Intuitive Surgical Inc. ("Intuitive") X and Xi EndoWrist products.

12. The facts and data I considered in connection with forming my opinions are identified in the body of this report and at the attached Attachment 2.

13. I am being compensated for my time spent in preparing this report at an hourly rate of $450/hr. If asked to testify in this lawsuit, I will be compensated at the rate of $450/hr for deposition testimony and $450/hr for testifying at trial. My compensation does not depend in any way on the outcome of this action.

IV. SUMMARY OF OPINIONS

14. The encryption on X and Xi EndoWrists requires substantially more computing resources to reverse engineer than the encryption of Si EndoWrists. Although the encryption techniques utilized by Intuitive for the use counters of the X and Xi EndoWrists can, and in fact have been, reverse engineered with adequate computing power and resources, as compared to the

encryption used for the use counter of the Si EndoWrists, the Xi encryption requires substantially more time and resources to reverse engineer.

15. Reverse engineering of the X and Xi EndoWrist encryption is simply a matter of computing power and financial resources. The time necessary to reverse engineer an X or Xi EndoWrist would be compressed with additional resources, and would have been possible within a similar time frame at least as early as 2019.

16. Intuitive's reason for employing encrypted communication between the X/Xi robots and the EndoWrists was to prevent modification of the use counter. The electronics within the Intuitive X and Xi EndoWrists do not actively control the EndoWrist, and third parties have only attempted to access or reverse engineer the use counter, not any other functionality of Si or X/Xi EndoWrists. Preventing third parties from accessing the use counter was Intuitive's primary concern when it selected the encryption used with Xi EndoWrists, and to this day Intuitive encrypts the communication of use counter data but does not encrypt communication of safety-critical patient sensor data.

V. ENCRYPTION OF X AND Xi ENDOWRISTS IS SUBSTANTIALLY MORE DIFFICULT TO REVERSE ENGINEER THAN Si, BUT IS NONETHELESS A MATTER OF AVAILABLE COMPUTING AND ENGINEERING RESOURCES

17. I understand that Intuitive Surgical, Inc. manufactures and sells surgical robots under the da Vinci brand name and related surgical attachments/instruments under the EndoWrist brand name. Specifically, there are multiple models or generations of commercial da Vinci robots and EndoWrists at issue here, including the Intuitive IS2000 designated "S", IS3000 designated "Si", IS4200 designated "X" and IS4000 designated "Xi" robots and their corresponding S/Si and X/Xi EndoWrist attachments.[12]

[12] Deposition of Anthony McGrogan at 15:14-20

18. Of particular interest is the use counter incorporated into both S/Si and X/Xi generations of robots and corresponding EndoWrist instruments. For both S/Si and X/Xi platforms, the use counter is designed to track the number of times a particular EndoWrist has been used in surgery. Each EndoWrist use counter is pre-programmed by the manufacturer (Intuitive), prior to delivery to the customer, with a limited number of uses or "lives".[13] According to Intuitive's Vice President of Design Engineering, Mr. McGrogan, in describing the use counters, "The Gen 3 Si/S instruments, those use a Dallas chip, which is a hard-wire connection.· And on Gen 4, which is X/Xi, we use an RFID counter."[14] It is my understanding based on technical documentation that I have reviewed that the actual use counter is solely designed to track the number of times an instrument has been used in surgery and report the remaining use count to the robot in order to display the number of "Uses Remaining".

19. In the Rebotix matter, I prepared and submitted an expert report entitled, "Expert Report of Kurt Humphrey," dated July 26, 2021 (my "Rebotix Report"). In the Rebotix Report, I opined regarding the technology and methodology that Rebotix would use to access and reset the Xi use counter. I have reviewed my Rebotix Report (attached as Attachment 3) and the documents considered therein (listed at the last page), and adopt and incorporate that Rebotix Report, including the opinions it represents and the identifications of documents and exhibits I reviewed, in its entirety herein.

20. In my Rebotix Report, I discussed the use counter of the Si EndoWrists and the security techniques used to prevent third parties from modifying that use counter. Rebotix Report at ¶¶ 12, 31-35.

[13] Deposition of Anthony McGrogan at 20:8-17
[14] Deposition of Anthony McGrogan at 77:18-20

21. In my Rebotix Report, I also discussed the use counter of the X and Xi EndoWrists and the encryption techniques used to prevent third parties from modifying that use counter. Rebotix Report at ¶¶ 19-30, 36-43.

22. As I noted in my Rebotix Report, "[t]he primary difference between the EndoWrist usage counter on the da Vinci S/Si EndoWrist and the da Vinci Xi EndoWrist is the manner in which the usage counter is accessed by the da Vinci system. For the S/Si instruments, the da Vinci system reads the data on the usage counter via a hard-wire connection, and for the Xi instruments, the da Vinci robot reads the data on the usage counter via an RFID counter."[15] Rebotix Report at ¶ 13.

23. The use counters of both S/Si and X/Xi EndoWrists are not based on anything about the use of the EndoWrist instrument during surgery, such as the time or amount of use during the surgery or forces incurred during surgery. In fact, although Intuitive measures, logs and stores detailed time-series logs of the torque on each of the motors and corresponding movement axes of the EndoWrists for both Si and Xi systems that would make such analysis possible,[16] it does not use this information in the use counter in any manner.[17]

24. On a da Vinci S/Si EndoWrist, the use counter is programmed into a Dallas Semiconductor chip hard-wired to the Gen 3 S/Si instrument. Specifically, a Dallas Semiconductor (DS) DS2505 16Kb Add-Only Memory chip is used in the S/Si EndoWrists. The DS2505 has three main memory components: a 64-bit lasered ROM, a 16384-bit EPROM Data Memory and a 704 bit EPROM Status Memory.[18] The S and Si instruments communicate with the

[15] Deposition of Anthony McGrogan at 77:12-23
[16] 30(b)(6) Deposition of Grant Duque at 13:11-18:23
[17] 30(b)(6) Deposition of Grant Duque at 18:25-19:10
[18] REBOTIX148555

EndoWrist via a one wire memory bus.[19] The DS2505 memory locations store the usage count data for the S and Si instruments. When the S/Si EndoWrist is connected to the da Vinci robot, the robot reads the data on the use counter through a hard-wire connection to determine how many uses remain on the counter. If the da Vinci robot reads that the EndoWrist has at least one use remaining, it will allow that EndoWrist to be used in surgery. In the event the use counter communicates that there are no uses remaining, the EndoWrist unit is rendered inoperable and the internal security key is deleted. According to Intuitive, "In comparison on IS3000 [S/Si robot] - ISI Key generated from Dallas unique id - key is needed for system to access Dallas data. When instrument is expired, key is wiped. All bits on dallas can only be 'cleared,' so once lives ticked off, cannot be reset."[20]

25. The da Vinci X/Xi robots and EndoWrists, on the other hand, communicate remaining use counts via RFID. An RFID system is a method by which data is communicated between two sources.[21] A RFID system consists of two components: tags and readers. A reader is a device that includes antennas that can emit and receive RF signals from a tag and optionally power a passive RFID tag. The tag uses RF signals to communicate information to a reader.[22] Unlike a hardwire connection, the RFID tag can transmit data without physically being connected to the RFID reader.[23] There are two types of tags—passive and active.[24] A passive tag is powered

[19] Deposition of Stan Hamilton at 143:12-144:7
[20] Intuitive: IS4000 8mm Base Instruments Final Design Review (FDR) Slide 192; Intuitive-00544903, at 00545094.
[21] https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification
[22] https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid
[23] https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification
[24] https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification

by the signal emitted from the reader.[25] An active tag is powered by a battery.[26] Each tag can store a range of information, from a single serial number to multiple pages of data.[27] An RF system for transmitting data does not affect the underlying stored data—it is a communication method for such data rather than a data storage system.

26. According to Intuitive's user manuals for the da Vinci X and Xi systems, each system uses RFID communication to detect installed instruments.[28] The RFID communication between the X/Xi robot and Xi EndoWrists operates at 13.56 MHz and complies with ISO/IEC 14443 Type B.[29]

27. X/Xi instruments include an Atmel CryptoRF interface with Atmel CryptoMemory security features. I have reviewed the CryptoRF EEPROM Memory Full Specification datasheet.[30] By default the CryptoRF has no enabled security, and operates as a simple RFID EEPROM memory.[31] Intuitive has confirmed that the RFID tags used in the X/Xi EndoWrist instruments are passive RFID tags and are powered by the RFID reader in the X/Xi system.[32] Contrary to the unencrypted hardwired data communications between the EndoWrist's Dallas chip and the S/Si robot, the user-configurable encrypted wireless data communications between the Atmel RFID

[25] https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid
[26] https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid, https://www.rfidjournal.com/faq/whats-the-difference-between-passive-and-active-tags
[27] https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid
[28] Intuitive Surgical da Vinci Xi System User Manual at E-16 (Intuitive-00002502 at 786) ("RFID communication is used by the da Vinci Xi system to detect and identify instruments and endoscopes that are installed on the system.") Intuitive Surgical da Vinci X System User Manual at E-11 (SIS357469 at 717) ("RFID communication is used by the system to detect and identify instruments and endoscopes that are installed on the system.")
[29] Intuitive Surgical da Vinci Xi System User Manual at E-17 (Intuitive-00002502 at 787), Intuitive Surgical da Vinci X System User Manual at E-12 (SIS357469 at 718)
[30] SIS357309 - Atmel CryptoRF EEPROM Memory Full Specificati,
[31] SIS357309 at 411
[32] 30(b)(6) Deposition of Grant Duque at 22:5-21

chip and the X/Xi robot are inherently more difficult to capture and decrypt. For example, one lead Intuitive engineer explained:

Q: And is it your understanding that there's different encryption used on the Si Dallas chip versus the Xi RFID chip?
A: That is correct.
Q. Is that the reason why at this time you believe that Xi is impossible?
A. That is correct.[33]

28. As Intuitive explained in its "Instrument Security Analysis" of December 2019, the respective security of the S/Si is "Low" compared to the "Medium" security utilized in X/Xi:[34]

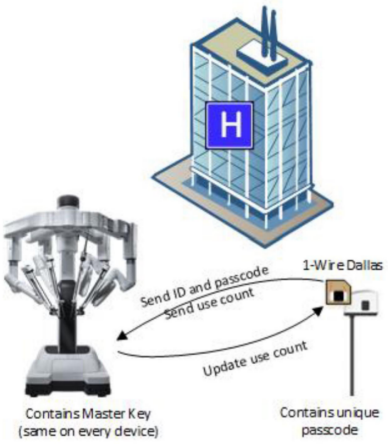
Product	Authentication chip	Interface	Counterfeit Auth Key	Use count	Security Level
Si	Dallas DS2505 (Production year ~1995)	1-wire	Passcode	OTP	Low
X/Xi/SP	Atmel AT88SC6416CRF (Production year ~2004)	RF	Secret Key	OTP	Medium

29. As Intuitive has explained, the main differences are that in the S/Si EndoWrists the "Communication Channel is not encrypted" and the "Master Key is hard coded and is not well protected in the system" whereas X/Xi EndoWrists have an "Authenticated and secure channel" and the "MasterKey is protected by CryptoCompanion":[35]

[33] Deposition of Shark Somayaji at 109:25-110:6
[34] Intuitive-01107582, at 583
[35] Intuitive-01107582, at 584-585

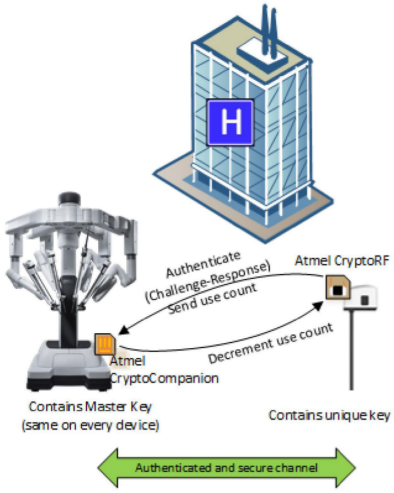
Si Instruments

- Authentication scheme
  - System has a Master Key (same key in every da Vinci)
  - Each instrument (Dallas DS2505) is programmed with a unique passcode derived from Master Key and instrument ID
  - During authentication, instrument sends its ID and the passcode to the system
  - System verifies the passcode by computing the expected value from the instrument ID and the Master Key
- Weaknesses
  - Communication channel is not encrypted. Scheme is susceptible to Replay and Man-in-the-Middle
    -> Capture a pair of (ID, passcode) and replay it on counterfeits
    -> Tamper with the traffic to send fake use counts
  - Master Key is hardcoded and is not well protected in the system
    -> Disclosure of Master Key (e.g., reverse engineering, data remanence, internal employees) allows one to easily program vanilla D2505 with right passcodes
  - Key /passcode length is short and brute-force is possible
  - Physical attacks to chips (e.g., UV, gamma) are possible



X/Xi/SP Instruments

- Authentication scheme
  - System has a Master Key (same key in every da Vinci) stored in CryptoCompanion
  - Each instrument (CryptoRF) is programmed with a unique key derived from Master Key and its instrument ID
  - During authentication, system sends a challenge (random number) and CryptoRF computes a response using its unique key
  - System receives the response and invokes CryptoCompanion to verify it using the instrument ID and the challenge.
  - The keys never leave CryptoCompanion or CryptoRF
- Weaknesses
  - Master Key is protected by CryptoCompanion, but *may* still be susceptible to invasive Physical attacks (microprobing, imaging)
    -> Disclosure of Master Key allows one to derive the CryptoRF keys
    -> Atmel reserved a certain ID range for ISI. This provides some assurance, but one could use custom hardware to emulate CryptoRF and use a valid ID within that range
  - UV/gamma attacks to reset use-count, but we use decrement-only
  - There are published Cryptanalysis and side-channel attacks
    -> Reveals only CryptoRF key. Still need to emulate a Tag to use the right ID
  - Communication channel is encrypted, but *may* still be susceptible to Replay and Man-in-the-Middle
    -> Encryption key used for use count and the rest of Cal data is the same. Copy-over from Cal data region.



30. These changes to the authentication and encryption methods used between the S/Si and X/Xi EndoWrists and systems substantially increase the amount of effort and computing power necessary to reverse engineer the X/Xi encryption, access and reset the use counter. Nonetheless, that does not mean that the X/Xi cannot be reverse engineered. For example, in October 2019, Intuitive was discussing third-party information that the Atmel "CryptoRF product

line we currently use is not as secure," which raised concerns about "about methods to reprogram our RFID's, i.e. change the life-count so that instruments get re-used beyond their design life."[36] As one of Intuitive's engineers explained when discussing this e-mail chain:

> Q. Do you have an understanding of what it would be referring to to be hacking the chip you use?
> A. Yes.
> Q. What's your understanding?
> A. My understanding would be trying to break into the RFID chip and the encryption. End of the day, these are all encryptions. So encryptions have a computer limit, right? Like, there is processing power that's needed, and you have to try combinations. And I am thinking they are saying there's an opportunity to hack into our RFID chip. Doesn't mean it's done, but that's true for all cryptography, right? Like, any encryption can be end of the day broken.[37]

31. In my original Report, I opined that "an image will be extracted from the Atmel CryptoRF chip on the X/Xi EndoWrists by Rebotix," that "based on Rebotix's past work with the S/Si EndoWrists and its understanding of the function of the usage counter, it will identify the usage counter in the extracted image," and that "Rebotix will have the capability to implement a reset of the usage counter on the X/Xi EndoWrists." Rebotix Report at ¶¶ 45-47.

32. Consistent with that opinion, Rebotix has now accomplished this from a technical perspective:

> Q. Has -- sitting here today, has Rebotix figured out how to circumvent the usage counter on Xi endoWrist instruments?
> MR. ERWIG: Objection. Form.
> THE WITNESS: Substantially, yes.
>
> * * *
>
> Q: So from a technical perspective today -- as of today, Rebotix has figured out how to reset the usage counter for Xi instruments. Is that what you're saying?
> MR. CORRIGAN: Objection. Asked and answered.
> MR. ERWIG: Same objection.
> THE WITNESS: I agree. Yes. I answered.

[36] Intuitive-00999771 (Ex. 220 to Deposition of Shark Somayaji)
[37] Deposition of Shark Somayaji at 123:2-17

BY MR. LAZEROW:
Q. Is the answer "yes"?
A. Yes. [38]

33. Also consistent with this opinion, Restore Robotics, another technology provider for the EndoWrist use counter reset, has created a reader for monitoring previously encrypted information of the EndoWrists, including the use count.[39]

34. Restore initiated a SOW for reverse engineering of the Xi EndoWrist interface with a third-party technology company in late June 2022,[40] reports having made substantial technical progress,[41] and expects to have a completed solution on the market in the third or fourth quarter of 2023.[42] This estimated schedule for completion is reasonable assuming that they continue to employ appropriate resources to the reverse engineering effort.

35. Restore and Rebotix's success is consistent with my personal experience in reverse engineering and Intuitive's statement that "any encryption can be end of the day broken" over time, and that "there is processing power that's needed, and you have to try combinations."[43] In other words, Intuitive's change in encryption techniques between S/Si and X/Xi didn't make reverse engineering impossible, it simply made it much more difficult, expensive and time consuming. This is consistent with the testimony of both Restore and Rebotix in reverse engineering X/Xi encryption:

Restore:
Q: Did that harm [caused by Intuitive] cause any delay to Restore's business?
MR. LAZEROW: Objection. Speculation.
THE WITNESS: Well, it absolutely caused delays and harm to our business. We had been counting on the revenues that we were generating from the repair business to fund

[38] Deposition of Stan Hamilton at 38:20-42:11.
[39] Deposition of Kevin May at 50:7-16.
[40] Deposition of Kevin May, Exhibit 155 at Restore-0091199; Kevin May at 51:6-53:1.
[41] Deposition of Kevin May at 89:10-25.
[42] Deposition of Kevin May at 60:9-25.
[43] Deposition of Shark Somayaji at 123:2-17.

being able to do additional R&D efforts, to grow the business, and to grow the Xi business and to do the research and development for the Xi.[44]

* * *

Q. What does finding the Crypto Companion chip mean for Restore's business as it relates to the X and Xi EndoWrists?

MR. LAZEROW: Objection.

THE WITNESS: It's just a -- a significant jump forward to be able to identify it and to be able to find that the -- the chip manufacturer. All those things were very positive. So it -- it -- it kind of shifts the -- kind of shifts the -- the -- the can we do this project to yes, we can do the project, but now it's just a matter of engineering, engineering, including time and money and effort. So it went from a nebulous idea of can we do this or can't we do this to yeah, we can do this. It's just a matter of engineering.

BY MR. MAIDA:

Q. How confident can you -- are you that Restore will be able to develop the technology to repair X- and Xi-compatible EndoWrists?

A. Extremely high.[45]

Rebotix:

Q. Okay. When did Rebotix start the process of trying to reset endoWrist Xi instruments?

A. I -- I can't give you a date on that because it started years ago in terms of beginning the process of looking into what the technology was, you know, things like understanding how the interface worked and what the challenges would be. That started years ago. The focus was on the Si, you know, to get out into the marketplace and actually see what happened, where we were at in the marketplace, and from a process development perspective that kind of thing, focus was on the Si. But looking into the Xi, that goes back years.

* * *

And so in that aspect there are delays, and also what point was there in investing all that money in moving forward if the same things that Intuitive was able to do to -- to suppress our business would have been done for the Xi also. Same story.[46]

36. In sum, Intuitive substantially increased the difficulty of reverse engineering the EndoWrist use counter from the S/Si EndoWrists to the X/Xi EndoWrists. Although this does not make reverse engineering of the X/Xi impossible, it makes it more difficult, time-consuming, and

[44] Deposition of Kevin May at 75:17-76:1.
[45] Deposition of Kevin May at 96:13-97:8.
[46] Deposition of Stan Hamilton at 42:11-44:12.

expensive. This reverse engineering work could have been performed at any time in the last five years, if not earlier, had the appropriate funding and resources been available.

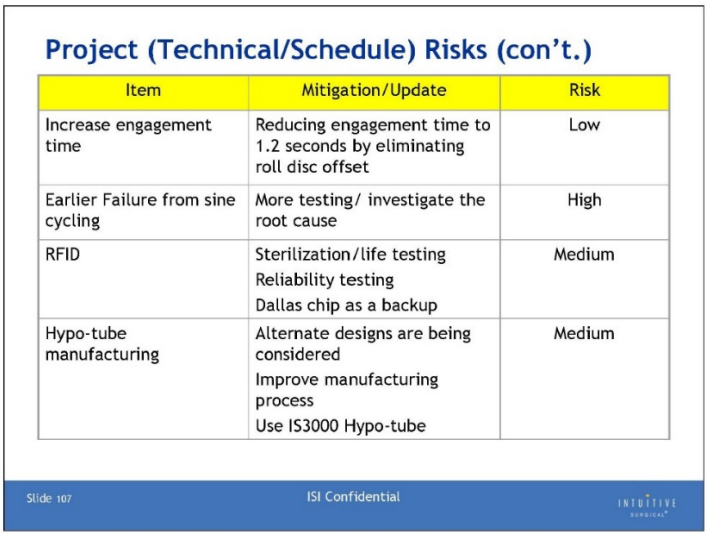
VI. INTUITIVE'S REASON FOR EMPLOYING THE MORE ROBUST ENCRYPTION AND SECURITY FEATURES FOR THE X AND Xi ENDOWRISTS WAS TO PREVENT MODIFICATION OF THE USE COUNTER

37. It is reasonable to explore Intuitive's possible motivation(s) in replacing the DS2505 EPROM with the Atmel CryptoRF EEPROM chip. After all, the old adage, "If it ain't broke, don't fix it" applies to complex systems, such as remote robotic surgical platforms, as much as it applies to other products including integrated circuit (IC) design, as demonstrated by the continued industrial interest in IP reuse. This philosophy is reflected in an excerpt from Exhibit 241, "Instruments for the S/Si and Xi platforms are similar in many regards. The materials used in the distal portion of the S/Si 8mm instruments are identical to those used in the equivalent versions of the Xi 8mm instruments."[47] The key factors in making significant design or component changes to any product are generally associated with performance/reliability, availability, and/or cost.

38. In terms of performance, evidence has not been identified indicating that the Atmel RFID chip offers any substantive improvement over the existing DS2505 chip in operational performance of the X/Xi system. On the contrary, any possible, yet unstated, performance advantages that might have been anticipated by introducing the RFID chip were insignificant enough that Intuitive used the conventional Dallas chip as their contingency or back-up plan in the event the RFID chip design change failed. Figure 1 from Exhibit 265, indicates that the "Project (Technical/Schedule) Risks" associated with the RFID chip introduction were considered

[47] Deposition of Grant Duque, Exhibit 241 at Intuitive-00027299

"Medium" and that Intuitive's RFID risk mitigation plan was to use the "Dallas chip as a "backup".[48] Figure 1 is reproduced below for reference.



Project (Technical/Schedule) Risks (con't.)

Item	Mitigation/Update	Risk
Increase engagement time	Reducing engagement time to 1.2 seconds by eliminating roll disc offset	Low
Earlier Failure from sine cycling	More testing/ investigate the root cause	High
RFID	Sterilization/life testing Reliability testing Dallas chip as a backup	Medium
Hypo-tube manufacturing	Alternate designs are being considered Improve manufacturing process Use IS3000 Hypo-tube	Medium

Figure 1

39. Moreover, another Intuitive slide from Exhibit 265 reproduced as Figure 2, below indicates that the X/Xi EndoWrist module was designed to use either the Dallas chip or the RFID chip without further modifications.[49] Therefore, it appears unlikely that the resulting EndoWrist operational or mechanical performance would be substantially different, or even distinguishable, regardless of which chip was used.

[48] 30(b)(6) Deposition of Grant Duque, Exhibit 265 at Intuitive-00542902 (Slide 107)
[49] 30(b)(6) Deposition of Grant Duque, Exhibit 265 at Intuitive-00542819 (Slide 24)

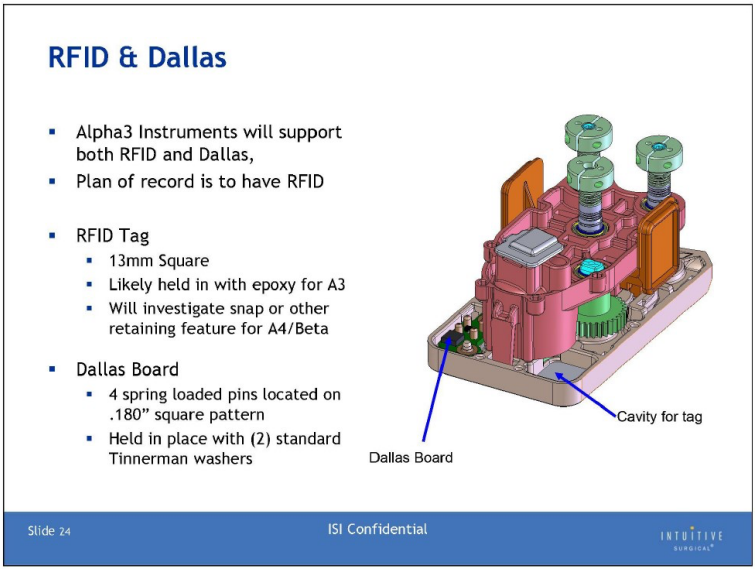


Figure 2

40. In terms of reliability, in reviewing the supplied the Intuitive documentation, there is no indication that a significant S/Si or EndoWrist instrument reliability issue associated with the Dallas chip was identified or addressed.

41. Moreover, a review of the disclosed comparative RMA/field failure data for the S/Si and X/Xi platforms provides no evidence of reliability issues associated with the DS2505 chip. Figure 3, the comparative "RMA Top Diagnoses by Rate" graphic from Exhibit 247, is reproduced below for reference.

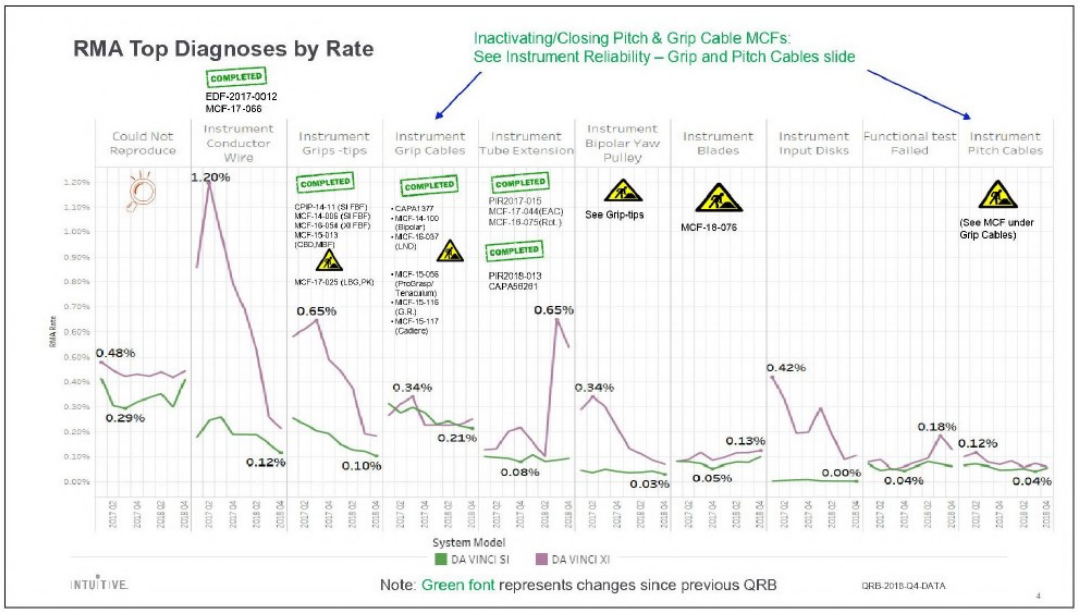


Figure 3

42. Although many factors can contribute to increased failure rates for a given product, it is interesting to note that Figure 1 shows 1) "Instrument Conductor Wire" failures were identified as the cause for a significantly higher Return Material Authorization (RMA) percentage for the "wireless" RFID Xi-EndoWrist instrument interface than for the "wired" Dallas Si-EndoWrist interface and 2) the return rate percentage for the Xi systems exceeds the return rate of the Si systems for essentially every RMA diagnosis. The disclosed RMA/return data details are insufficient to draw any firm conclusions regarding reliability issues associated with replacement of the DS2505 chip in the S/Si EndoWrist instruments with the Atmel CryptoRF chip in the X/Xi EndoWrist instruments but the results suggest that improved reliability was not a key factor or motivation in redesigning the X/Xi robot-EndoWrist interface.

43. In terms of availability, there is no evidence I am aware of indicating that the DS2505 device supply or availability was limited at the time of the X/Xi system design/development or would become threatened in the foreseeable future. On the contrary, as

discussed previously, the availability of Dallas chips was sufficient for Intuitive to plan to use the "Dallas chip as a backup" to mitigate risks associated with the development of the RFID interface for the X/Xi platform. Moreover, lack of adequate DS2505 chip supply would be particularly unlikely considering the relatively small number of DS2505 chips required to support typical S/Si and X/Xi EndoWrist production volumes. Therefore, migrating the DS2505 device from the S/Si platform to the X/Xi platform should have been relatively straightforward from an availability standpoint.

44. That leaves cost as the most likely motive for Intuitive to take on the substantial task of redesigning the X/Xi robot-EndoWrist interface. There are a variety of costs that can motivate businesses to consider redesigning their products. Three of the most common commercial costs are material, production, and opportunity, i.e. those impacting revenue or profit.

45. In the case of the S/Si and X/Xi systems, material cost is highly unlikely to be a factor in switching from the Dallas chip to the Atmel CryptoRF chip, since the difference in material costs of these commodity ICs is undoubtedly negligible compared to the cost of a da Vinci system and EndoWrist instruments used with the system.

46. Likewise, the difference in production cost associated with using either the Dallas chip or the Atmel RFID chip is also undoubtedly negligible. For example, Figure 2 above indicates the wired (Dallas) chip and wireless (RFID) chip are essentially interchangeable between the S/Si or X/Xi platforms. On the contrary, Intuitive documentation indicates that programming of the RFID chip requires special tooling that is not required for the programming of the Dallas chip.

47. Therefore, if reduced material costs and production costs are unlikely motivations to undertake the considerable effort/cost and risks associated with redesigning the X/Xi-EndoWrist interface, then one must consider opportunity costs as a possible motivation.

48. Review of the supplied Intuitive documentation sheds considerable light on the opportunity costs associated with redesigning the S/Si and X/Xi-EndoWrist instrument interface, namely in addressing lost revenues associated with used EndoWrist instrument repair and reprocessing by third-parties. For example, Intuitive's concern regarding third-party repair/reprocessing of used tools as it relates to the incorporation of the RFID chip is clearly evident an internal email entitled "RFID Team Action Items"[50]. The email begins with the statement,

> "In my initial thoughts on this, there are two threats we're worried about:
>
> 1. Reprocessing: Take an expired instrument and restore its available lives
> 2. Counterfeiting: Take a non-ISI-designed instrument and put valid data on a tag so that it is accepted by our machine.
>
> We'd like to make both of these difficult with the security features on our tag. Reprocessing seems the more likely threat."

(Emphasis added).

49. Another excerpt from this same email, discussing Intuitive's primary concern of stopping additional lives from being added, states:

> The unique id doesn't prevent reprocessors from putting lives back on our instruments. In principle, you could copy the blob of data off a new instrument, then put that same blob of data back on once it's expired, and it will be as good as new. I believe the Dallas implementation uses a "write once" region in the tag to ensure that decremented lives stay decremented.

[50] 30(b)(6) Deposition of Grant Duque, Exhibit 267 at Intuitive-02068695-97.

(Emphasis added).

50. The "RFID Team Action Item" email continues by explaining that this is a reason to go with the Atmel solution:

> "It seems to me that we want something to physically change in the tag (e.g., blowing a fuse) as we expire lives in the instrument. We do have something like that from Atmel. If we can't get it from Baylogh's tag suppliers, we would leave a pretty significant vulnerability."

(Emphasis added).

51. Intuitive's focus on using the Atmel chip for purposes of preventing the addition of more lives to the EndoWrists is demonstrated by another e-mail during early Xi EndoWrist development, in which an Intuitive lead engineer for "architectural decisions" and "high-level 2 strategy for design" for Xi[51] stated the sole concern as preventing addition of lives to the EndoWrist: "We need to at least make sure that someone can't just copy the contents of a tag from a new instrument and reprogram it at the end of life with the same information."[52]

52. Intuitive's sole focus during encryption development on the use counter, and the opportunity cost of introducing encrypted communications for the use counter data is validated, for example, by Intuitive's decision to phase out S/Si instruments, which was implicitly acknowledged to be to protect instrument revenue because " companies have so far only done reprogramming on Si." and "And we probably have lead time before they figure out X/Xi." as the reprogramming had not yet been reverse engineered for X/Xi:[53]

[51] 30(b)(6) Deposition of Grant Duque at 26:4-27:3
[52] 30(b)(6) Deposition of Grant Duque, Exhibit 266 (Intuitive-02068686)
[53] Intuitive-01019873

From: Katie Scoville [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=015E406D44CF40CDABB530EFD918CA54-KATIE SCOVI]
Sent: 5/7/2018 12:31:46 PM
To: Ryan Shaw [Ryan.Shaw@intusurg.com]
Subject: reprogrammed instruments and Si portfolio

Ryan,

Just thinking…the emergence of 3rd party reprogramming is another possible reason to move away from Si. The companies have so far only done reprogramming on Si. IF, they figure out Xi we have the ability to respond with SW much faster. And we probably have lead time before they figure out X/Xi. I don't think the slides need updating, but it is something to think about.

Thanks,
Katie

Katie Scoville
Director Product Marketing, Secondary Markets
Office: +1 (408) 523-7562 Cell: +1 (408)628-8323
katie.scoville@intusurg.com

53. Therefore, the opportunity cost associated with a redesign of the X/Xi-EndoWrist interface using an encryption-capable RFID chip that will be more difficult to reset (such as by using the Rebotix Interceptor Assembly or similar technology), represents a substantial increase in Intuitive Surgical revenues. This would appear to be the strongest motivation to redesign the existing Dallas chip-based interface with the Atmel RFID interface.

54. Consistent with Intuitive's focus on preventing the addition of lives during X/Xi encryption development, Intuitive agrees that third parties have only ever attempted to access or reverse engineer the use counter.[54] Intuitive documentation and testimony indicate that third-parties have successfully reverse engineered, or attempted to reverse engineer, the S/Si and X/Xi robot/EndoWrist interfaces solely for the purpose of resetting the use counter to extend the life of the instrument.

[54] 30(b)(6) Deposition of Grant Duque at 34:2-35:22; Deposition of Shark Somayaji at 110:7-112:10

55. Indeed, in October 2019, when Intuitive received third-party information that the Atmel "CryptoRF product line we currently use is not as secure," the only concerns they raised were "about methods to reprogram our RFID's, i.e. change the life-count so that instruments get re-used beyond their design life"[55] – in other words, Intutive was unconcerned about any other data stored on the RFID chip.

56. When recently given the opportunity to select between multiple encryption and connectivity techniques for different types of data, Intuitive chose stronger RF encryption for its use counter while using less robust encryption methods for critical sensor data used to provide haptic feedback to surgeons. As described by a lead Intuitive engineer, the feedback data is "exceptionally important" yet is not transmitted via the RFID interface:

Q. I'd like to ask a few more questions about Skywalker instruments. So I understand that there's forced feedback in Skywalker instruments, correct?
A. That is correct.
Q. And then there's some sort of signal that gets transmitted out through the instrument to the robot?
A. That is correct.
Q. And that in turn gets processed and provided to the surgeon via the surgeon's console?
A. That is correct.
Q: Are the – that signal – call it a forced feedback signal -- does that forced feedback signal get transmitted out of the instrument via the RFID chip?
A. No, it does not.
Q. And I guess a question we might establish first, is there an RFID chip in Skywalker instruments?
A. Yes, there are.
Q. So how does the forced feedback signal in Skywalker instruments get transmitted out from the instrument to the robot?
A. In case of Skywalker instrument, the forced feedback signal is transmitted through a different mechanism, it's a pogo pin.
Q. A pogo pin. So that's a physical electrical connector between the instrument and the robot
A. That is correct.
Q. Is there any sort of chip or anything inside of the instrument that's involved in the transmission of the forced feedback signal?

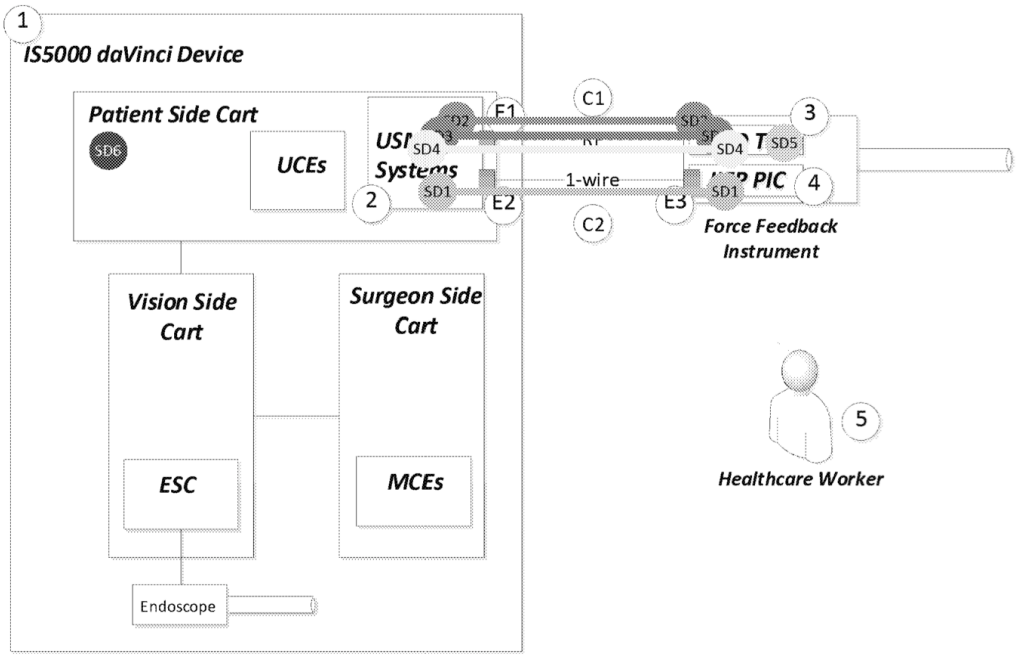
[55] Intuitive-00999771 (Ex. 220 to Deposition of Shark Somayaji)

A. Yes, there is.
Q. What is that chip called?
A. I don't think that chip has a name. It is a PCB with several components.
Q. And by "PCB," you mean a printed circuit board?
A. That is correct.
* * *
Q. Why would there need to be security for the PIC?
A. Good question. So forced feedback instruments, so they are supposed to provide feedback to the surgeon when -- when there is X, Y or Z forces that are showing up, so they have to be fed back to the surgeon. So you want that feedback to be accurate and never tampered with and the surgeon is trying to generate, let's say five pounds of force and the signal is tampered to, let's say, show only a tenth of the force, he's going to push harder to get the five pounds, and in turn he's injured the patient. So it's exceptionally important that the signal here be not tampered by anybody.[56]

57. Yet, despite the "exceptional importance" of not having this signal tampered with, Intuitive's "Cybersecurity System Architecture" provides minimal security to the force feedback data, or the connections that provide that data to the system, and via the system, to the surgeon. For example, the data connection between the force feedback sensors and the system is labeled "C2" and "SD1" in the depiction below:[57]

[56] Deposition of Shark Somayaji at 132:8-138:2
[57] Deposition of Shark Somayaji, Exhibit 228 at Intuitive-01004232, at 238.

4.7 Sensitive Data Flows (visual diagram)



58. However, this connection is left largely unprotected, particularly when compared to the "Instrument Use Count Data":[58]

4.8 Sensitive Data Flow and Location Table

ID	Sensitive Data Flow Name	Type(s) of Data	PHI/PII Present?	Protected? (Confidentiality)	Protected? (Integrity)	Protected? (Authenticity)	List all Cache / Storage Locations
SD1	Force Feedback Sensor Data	Data collected from physical sensors on the instrument	No	No	Yes (CRC employed)	No	2, 4
SD2	Force Feedback instrument calibration data	Data used for correctly calibrating instrument force feedback functionality	No	Yes	Yes	Yes	2, 3
SD3	Instrument configuration and identification data	Unique instrument id, version, type, and name stored in protected area of secure RFID tag	No	Yes	Yes	Yes	2, 3
SD4	Instrument use count data	Usecount data stored in protected area in secure RFID tag	No	Yes	Yes	Yes	2, 3
SD5	Instrument Authentication Key	Key used for authentication of an instrument to the system	No	Yes	Yes	Yes	3
SD6	Instrument Rootkey	Rootkey for driving instrument specific authentication keys	No	Yes	Yes	Yes	1

[58] Exhibit 228 at Intuitive-01004232, at 236, 239.

4.4 Reference System Architecture - Communications Path Table

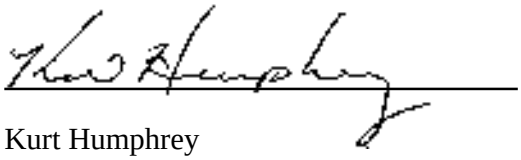
ID	Transport Layer Protocol Name	Application Layer Protocol Name	Protected? (Confidentiality)	Protected? (Integrity)	Protected? (Authenticity)	Sensitive Data	Ref Arch Endpoints	Role
C1	RF	Custom, proprietary	Yes	Yes (employs CRC)	Yes	Yes (instrument configuration, instrument use count, instrument calibration)	2(E1), 3	Communication link between instruments and USM
C2	1-wire	Custom, proprietary	No[1]	No[1]	No[1]	No	2(E2), 4	Supply power to IIFP PIC and transfer information through 1-wire interface

59. In sum, since the initial design of the encryption for the X/Xi EndoWrists in the early 2010s, Intuitive's driving concern with encryption has been to prevent extension of the number of instrument lives. Consistent with this driving concern, none of the other data stored within an EndoWrist has ever been accessed, and indeed, Intuitive admits that it would make no sense to access this other data. Intuitive's primary concern of stopping third-parties from adding lives to EndoWrists with X/Xi RFID encryption is further confirmed by the fact that it continues to use similar encryption for its next generation of products, while not protecting the most critical data that directly affects patient safety to the same extent.

VII. CONCLUSION

60. On balance, the Intuitive documentation and testimony I reviewed describing the design and development of the X/Xi-EndoWrist interface and the corresponding change from a wired, unencrypted Dallas chip (EPROM) to the wireless, encryption-enabled Atmel CryptoRF chip shows a deliberate attempt on the part of Intuitive to thwart efforts by third-parties to reset the instrument's use counter. Extending the field life of Intuitive's EndoWrist instruments, regardless of robotic platform, negatively impacts instrument sales resulting in a significant loss in revenue. Intuitive has been shown to have incurred additional design risks and costs in their development of the X/Xi robotic surgical platform and associated EndoWrist instruments in a

deliberate effort to thwart the instrument service providers' ability to reset the instruments' use counters and thereby extend the life of EndoWrist instruments.



Kurt Humphrey

December 2, 2022

ATTACHMENT 1

***Curriculum Vitae* of Kurt Humphrey**

Kurt D. Humphrey

Semiconductor Fabrication, Processing, and Chemical/Materials Expert

After graduating with his B.S. in Ceramic Engineering, Mr. Humphrey accepted a Product Development engineering position with General Motors' AC Spark Plug division where he developed and patented the seminal process for physical vapor deposition (PVD) of Pt catalytic coatings on partially-stabilized zirconia oxygen sensors for state-of-the-art automotive emission control systems. Kurt was subsequently awarded a GM Graduate Study Fellowship and continued research in the area of automotive electronics with the development of **novel methods for fabricating multilayer ceramic capacitors** and other piezoelectric components through funding by General Motors Research Laboratories. After completing his M.S. degree in Ceramic Engineering, Kurt joined Delco Electronics (Delphi) Division of General Motors where he led process development and engineering in the areas of Czochralski (Cz) single-crystal silicon growth and semiconductor device/IC fabrication for bipolar, MOS, and silicon MEMS (MAP sensor) products.

Mr. Humphrey's expertise in materials and microelectronics subsequently led to assignments as Thin Films Process Development Manager where he developed and transferred to production the PVD tantalum salicide (TaSi) process used in AT&T's and Bell Labs' DRAM memory products. Kurt subsequently served as Submicron Process Integration Manager at N.V. Philips Research Laboratories in Eindhoven, NL including development of next-generation wafer cleaning, isolation, contact plug, via metallization and ILD gap-fill processes for state-of-the-art semiconductor device production. While at Philips, Kurt collaborated with engineers at AMD, Intel, TSMC, Texas Instruments, and Siemens on advanced materials development and IC process/fabrication technology through formal technology transfer agreements between the companies.

Mr. Humphrey came to Colorado Springs as Process Integration Manager for United Technologies Microelectronics Center (UMTC) developing and patenting state-of-the-art radiation-hardened triple-level metal (TLM) CMOS, programmable amorphous silicon anti-fuse, and deep-trench fully-isolated, complimentary bipolar silicon-on insulator (SOI) process technologies. Kurt transferred to Rockwell Semiconductor Systems/Conexant where he served as Advanced Process Integration Manager for 90nm CMOS pilot production. Later, with Rockwell and Conexant, Kurt developed and patented a commercial stiction-free wet etching process for releasing bulk micro-machined MEMS resonating structures used in state-of-the-art MEMS gyroscopes. During his long tenure in the industry, Mr. Humphrey worked with key semiconductor equipment and materials vendors including Applied Materials, Advantest, ASML, Ericsson, Huawei, JSR, Nokia, LAM, Novellus, ULVAC, SOITEC, Shin Etsu (SEH), Sumitomo, Teradyne and many others to develop and characterize next-generation microelectronic components, designs, and fabrication technologies.

Kurt has spent the past 22 years as a full-time IP technologist and subject matter expert (SME) in microelectronics and wireless telecom technologies. Kurt has served as a consulting and/or testifying expert in multiple lawsuits including an **ITC patent infringement case between HP and Acer** and **provided trial testimony as the expert for the plaintiff (the Houston Rockets organization) v. iLight Technologies in a 2012 product liability case involving LED lighting technology in 2012**. The jury found for the Plaintiff. Most recently, Kurt has provided expert analyses, reports and declarations in support of wireless telecom IPRs instituted by the USPTO's Patent Trial and Appeal Board (PTAB). Mr. Humphrey has been engaged numerous times to provide forensic/reverse engineering services and subject matter expertise primarily in the areas of commercial and industrial electronics and high-tech materials, and has analyzed literally thousands of patents and countless patent portfolios for clients in the Global High-tech Top 100.

In addition to his consulting work, Mr. Humphrey currently serves as Adjunct Professor of Chemistry in the College of Engineering at Colorado Technical University teaching inorganic and organic chemistry.

3780 Masters Drive, Colorado Springs, CO 80907· tel: +1-719-331-9788 · fax: +1-719-260-0580

PROFESSIONAL EXPERIENCE

IP *Enginuity* LLC. **2005-Present**

Managing Director/Principal Technologist

- Comprehensive Engineering Services Provider for the Intellectual Property and Patent Asset Management, Licensing, Litigation and Technology Transfer Industries.
- Prepare strategies and manage engineering services relating to IP asset and patent evaluation; reverse/forensic engineering and re-engineering; patent enforcement, assertion and licensing; portfolio mining; prior art searches; technology transfer; and IP litigation support.
- Primary technical contributor on projects relating to MCT/CZT IR focal plane arrays for the United Technologies Science Center, semiconductor devices and advanced/engineered materials including forensic and patent infringement investigations into LED lighting systems, LED phosphors, and solid-state DFB laser devices, organic LEDs (OLEDs) and optical networking components, protocols and standard essential patents (SEPs), consumer electronics, RFID, photonics and opto-electronic devices; MEMS and sensors; flat panel displays (FPDs), and biotech/medical products and systems.
- Expert witness experience in patent infringement, trade secret and antitrust litigation.

TAEUS International Corp. **1999 – 2005**

Director, Engineering Services

- Managed patent evaluation and reverse engineering projects from the initial proposal through project completion and final review.
- Serve as a primary technical contributor/SME on wireless telecom/networking standards incl. 802.11, Bluetooth and 3G/4G cellular and associated SEPs, optical networking and opto-electronic/photonics components including collaboration with Dartmouth and HP scientists to measure and characterize non-linear optical effects in commercial optical fibers. Also as an SME on a variety of compound semiconductor devices, solid state DFB/quantum well lasers, photonics/opto-electronics components, FPD technologies, e.g. LCD, plasma and LED/OLED, , MEMS, sensors,) etc. and biotech related projects.
- Specific responsibilities include client interface, project definition, cost, resource and schedule planning, technical input, supervision of staff engineers, external consultants and labs, patent evaluation, claim chart construction, and technical report writing.
- Clients included many Global 100 high tech companies and leading U.S. patent law firms.

Rockwell Semiconductor Systems/Conexant Systems **1995 - 1999**

Advanced Process Development Manager

- Assess new business opportunities, perform technical audits and generate comprehensive business and financial plans for review and approval by Rockwell CEO and senior staff.
- Primary focus on state-of-the-art semiconductor products e.g., Power-Trench Diodes and Trench IGBTs, CMOS imagers and MEMS gyros.
- Coordinate design rules, mask/reticle specifications, test chip design/layout, process qualification and transfer to production for 90nm CMOS process development in Rockwell's Advanced Process Technology (APT) department in Newport Beach.

Process Integration Manager

- Demonstrated first fully-functional Trench IGBTs and silicon MEMS gyro using 125mm substrates.
- Authored 3 MEMS and 1 SAW filter disclosures; 1 MEMS patent issued, others pending.
- Successful completion of comprehensive STI and 90nm CMOS process development test chips in record time to support an aggressive 90nm qualification schedule.

United Technologies Corp. (UTMC) **1989 – 1995**

Process Integration Manager

- Direct next-generation CMOS and bipolar process technology development. Development projects included: ACUTE (advanced dielectrically-isolated, complementary bipolar linear array process on SOI), UTERPROG (radiation-hardened 1.0µ CMOS PAL technology utilizing vertical amorphous Si antifuses), and UTERTLM (1.0µ triple-level metal, rad-hard CMOS)
- Developed advanced amorphous silicon metal-to-metal antifuse technology to support 256k RHPROM and RHPAL field programmable products; 2 patents issued.
- Developed novel trench-isolated, complementary bipolar SOI process, 1 patent issued

Philips Research Labs (Eindhoven, The Netherlands) **1986 – 1989**

Process Integration Manager

- Direct development of 0.7µ CMOS process from R&D phase through final product qualification as part of the Philips/Siemens "Mega" project. Project deliverables included commercial 1M SRAM and 4M DRAM products.
- Directed activities of 10 senior technologists.
- Developed first sub-micron CMOS process utilizing retro-wells, suppressed-BB LOCOS, salicide with $TiSi_2$ local interconnect, W plugs and I-line lithography.
- Integration team produced Philip's first fully-functional 1M SRAM using state-of-the-art 0.7µ CMOS process (C1DM)

AT&T Technologies **1983 – 1986**

Process Engineering and Yield Enhancement Manager

- Coordinate DRAM process transfer from R&D to fab, and direct yield enhancement activities for 256k DRAM production in new 125mm line (KC-1).
- Section Leader for Thin Films/Ion Implantation Engineering
- Key contributor in successful start-up of new 125 mm high volume memory fab (KC-1);
- Representative on corporate committee for thin film metallization processes and invited speaker at SEMI/ASTM meeting on PVD target specifications.

DELCO Electronics Div. General Motors **1980 – 1983**

Process Development Engineer (Silicon Crystal Growing, Bipolar and MOS Fabs)

- Provide production engineering support, initially for Si crystal growing area, and later for MOS diffusion and LPCVD areas
- Evaluated external silicon wafer suppliers and introduced intrinsic-gettered substrates into MOS fab resulting in an average 7% increase in die yield across all devices

AC Spark Plug Div., General Motors **1978 – 1980**

Associate Process Development Engineer

- Developed process for depositing Pt catalytic thin films onto partially-stabilized zirconia oxygen sensors
- Key investigator and inventor on U.S. patent: "Electrode Sputtering Process for Exhaust Gas Oxygen Sensor"
- 1979 GM Graduate Study Fellowship Award

EDUCATION and ACADEMIA

M.S. Ceramic Engineering, University of Missouri - Rolla
B.S. Cum Laude, Ceramic Engineering, University of Missouri – Rolla
Adjunct Professor of Chemistry in the College of Engineering at Colorado Technical University-Colorado Springs - Current

U.S. PATENTS:

6,337,027 Microelectromechanical device manufacturing process
5,759,876 Method of making an antifuse structure using a metal cap layer
5,658,819 Antifuse structure and process for manufacturing the same
5,344,785 Method of forming high speed, high voltage fully isolated bipolar transistors on a SOI substrate
4,253,931 Electrode sputtering process for exhaust gas oxygen sensor

HONORS

General Motors Graduate Study Fellowship – 1979
United Technologies Silver Quill Award – 1994
Rockwell Outstanding Achievement Award – 1998

PROFESSIONAL MEMBERSHIPS

Institute for Electrical and Electronics Engineers (IEEE) / Electron Devices Society
Colorado Photonics Industry Association
Licensing Executive Society (LES)
Intellectual Property Owners Association (IPO)
Society for Optical Engineering (SPIE)
Intellectual Asset Management (IAM)

Expert Litigation Case History (Partial)

2007 – ITC Case No. 337-TA-606, *Hewlett Packard (Plaintiff) v. Acer International*:
Provided expert reverse engineering services, expert report and deposition for the Plaintiff

2012 – District Court 157th Judicial District Harris County Texas Cause No.2009-76645, *Clutch City Sports and Entertainment a.k.a. Houston Rockets (Plaintiff) v. iLight Technologies*:
Provided expert failure analysis services, expert report, deposition and trial testimony for the Plaintiff. Jury chose in favor of the Plaintiff.

2018 – IPR Case IPR2017-001889 before the USPTO PTAB, *Sprint Spectrum v. General Access Solutions (Patent Owner)*:
Provided expert declaration and was deposed on behalf of the Patent Owner

2020 - IPR Case IPR2019-01668 before the USPTO PTAB, *Samsung Display (Petitioner) v. Solas OLED (PO)*: Provided expert declaration in support of the Patent Owner

2021 – Western District of Texas Civil Action No.: 6:20-cv-879 (ADA), *Proxense LLC (Plaintiff) v. Target Corp.*: Provided expert declaration and deposed on behalf of the Plaintiff

2021 - Middle District of Florida, Tampa Division, Case No. 8:20-cv-02274, *Rebotix Repair LLC (Plaintiff) v. Intuitive Surgical, Inc.*:
Provided expert report and expert deposition on behalf of Plaintiff

2021 – Southern District of Iowa Central Division, Case No. 4:19-cv-00330-RGE-CFB, Neogen Corp. v. Innovative Reproductive Technology LLC: Provided expert report, scheduled for trial testimony in June

2022 – IPR Case IPR2021-00929 (US 7,080,330) before the USPTO PTAB, *Western Digital Technologies, Inc.(Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration and was deposed on behalf of the Patent Owner

2022 – IPR Case IPR2021-01339 (US 8,686,538) before the USPTO PTAB, *Applied Materials, Inc.(Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration and was deposed on behalf of the Patent Owner

2022 – IPR Case IPR2021-01340 (US 6,725,402) before the USPTO PTAB, *Applied Materials, Inc.(Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration and was deposed on behalf of the Patent Owner

2022 – IPR Case IPR2021-01342 (US 6,968,248) before the USPTO PTAB, *Applied Materials, Inc.(Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration and was deposed on behalf of the Patent Owner

2022 – IPR Case IPR2021-01344 (US 6,907,305) before the USPTO PTAB, *Applied Materials, Inc.(Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration and was deposed on behalf of the Patent Owner

2022 – IPR Case: IPR2021-01349 (US 6,420,097) before the USPTO PTAB, *ST Microelectronics, Inc. (Petitioner) v. Ocean Semiconductor LLC (Patent Owner)*: Provided expert declaration on behalf of the Patent Owner.

ATTACHMENT 2

List Of Materials Cited

The following materials were used in forming my opinions:

1. Email thread beginning on December 10, 2021, filed as Doc. 180-1, Rebotix Repair, LLC re Document Number CPT2000126
2. Intuitive-00002502
3. Intuitive-00027298
4. Intuitive-00027299
5. Intuitive-00027622-24
6. Intuitive-00027843
7. Intuitive-00027844-46
8. Intuitive-00089606-08
9. Intuitive-00105113-18
10. Intuitive-00194931-35
11. Intuitive-00214902-03
12. Intuitive-00290826-31
13. Intuitive-00506505-641
14. Intuitive-00512348-53
15. Intuitive-00542796-919
16. Intuitive-00544903-5124
17. Intuitive-00552745-59
18. Intuitive-00555960
19. Intuitive-00556188-90
20. Intuitive-00556193-95
21. Intuitive-00556951-53
22. Intuitive-00560955-56
23. Intuitive-00561044-49
24. Intuitive-00561050-55
25. Intuitive-00593443-80
26. Intuitive-00602553-56
27. Intuitive-00602580
28. Intuitive-00602581
29. Intuitive-00602758-59
30. Intuitive-00602760-79
31. Intuitive-00671020-35
32. Intuitive-00960492-95
33. Intuitive-00967509
34. Intuitive-00967510-42
35. Intuitive-00967590

36. Intuitive-00967609-13
37. Intuitive-00967614-34
38. Intuitive-00988310-16
39. Intuitive-00990665-66
40. Intuitive-00991239-40
41. Intuitive-00991241-42
42. Intuitive-00994614-17
43. Intuitive-00999076
44. Intuitive-00999252-68
45. Intuitive-00999731-42
46. Intuitive-00999734
47. Intuitive-00999771-75
48. Intuitive-01001554-55
49. Intuitive-01002987-89
50. Intuitive-01004230-31
51. Intuitive-01004232-39
52. Intuitive-01005095-96
53. Intuitive-01019873
54. Intuitive-01031408-11
55. Intuitive-01085683-85
56. Intuitive-01095425-29
57. Intuitive-01107582-88
58. Intuitive-02066979-7059
59. Intuitive-02067770-72
60. Intuitive-02068686
61. Intuitive-02068695-97
62. REBOTIX148555-78
63. REBOTIX175417
64. REBOTIX175468
65. REBOTIX175710
66. Restore-00001248-56
67. Restore-00091199-206
68. Restore-00091362
69. Restore-00094918-56
70. SIS357469-812
71. SIS357309-468 - Atmel CryptoRF EEPROM Memory Full Specification
72. Expert Report of Kurt Humphrey, submitted in the matter of Rebotix Repair LLC v. Intuitive Surgical, Inc., Case No. 8:20-cv-02274 (M.D. Fla.) and dated July 26, 2021
73. Interview with Stan Hamilton on Juley 23, 2021
74. Deposition of Anthony McGrogan dated June 7th ,2021

75. Deposition of Stan Hamilton dated June 4, 2021
76. Expert Report of Gwen Mandel dated July 26, 2021
77. Fukami, Aya, et al., A New Model for Forensic Data Extraction from Encrypted Mobile Devices, Forensic Science International: Digital Investigation, Elsevier, May 27, 2021, www.sciencedirect.com/science/article/pii/S2666281721000779.
78. Conti, Gregory, et al., Visual Reverse Engineering of Binary and Data Files, Visualization for Computer Security Lecture Notes in Computer Science, Sept. 2008, pp. 1–17., doi:10.1007/978-3-540-85933-8_1.
79. A. Amsler and S. Shea, RFID (Radio Frequency Identification), TechTarget, https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification
80. 30(b)(6) Deposition of Grant Duque dated November 8, 2022
81. Exhibit 264 to the 30(b)(6) Deposition of Grant Duque dated November 8, 2022
82. Exhibit 238 to the Deposition of Grant Duque dated November 8, 2022
83. Deposition of Grant Duque dated November 8, 2022
84. Deposition of Sharathchandra “Shark” Somayaji dated November 4, 2022
85. Deposition of Kevin May dated November 3, 2022
86. Deposition of Stan Hamilton dated November 4, 2022

ATTACHMENT 3

Expert Report of Kurt Humphrey in *Rebotix Repair LLC v. Intuitive Surgical, Inc.*, Case No. 8:20-cv-02274 (M.D. Fla)

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

REBOTIX REPAIR LLC, Plaintiff, vs. INTUITIVE SURGICAL, INC., Defendant.	Case No. 8:20-cv-02274 HIGHLY CONFIDENTIAL INFORMATION - ATTORNEYS' EYES ONLY

EXPERT REPORT OF KURT HUMPHREY

TABLE OF CONTENTS

I. INTRODUCTION

A. Qualifications

1. I currently work as Managing Director and Principal Technologist at IP Enginuity LLC. I have held that position for the past 15 years.

2. I hold B.S. and M.S. degrees in Ceramic Engineering from the University of Missouri-Rolla and worked primarily as a Process Development Engineer and Process Integration Manager during my 20+ year history in integrated circuit (IC) device and smart sensor processing. My professional experience in industry included responsibilities for complementary metal oxide semiconductor (CMOS) process development for DRAM, SRAM, EEPROM and SONOS flash and embedded non-volatile (NV) memories at AT&T Technologies, Philips Research Laboratories in Eindhoven, NL, and United Technologies Microelectronics Center. While at Philips, I collaborated with engineers at Siemens (DE), IBM (US), Intel (US), Motorola (US), Texas Instruments (US) and SEMATECH (US) on next-generation memory technology through formal technology transfer agreements with Philips (NL).

3. I am an expert in reverse engineering (RE) industrial and consumer microelectronic devices, components and systems including RFID products such as smart EMV smartcards and other proximity integrated circuit cards (PICCs). Over the course of my career, I have reverse engineered a large number and wide variety of semiconductor devices including microprocessors and non-volatile memories such as EEPROMs and Flash products for OEMs such as Apple, Alcatel-Lucent (Nokia) and others.

4. I have been engaged by multiple clients to extract or "dump" contents of specific EEPROMs and flash memories used in contactless RFID smart cards such as Visa payWave, Gemalto and other contactless EMV cards. The primary objective was to analyze the code or firmware with respect to patent enforcement/infringement matters.

5. I have general familiarity with encryption and security used in RFID communications, including encryption via stream ciphers and mutual authentication protocols.

6. I have been deposed as a technical expert four times and provided expert trial testimony in a product liability case.

a. I was engaged as an expert in an International Trade Commission (ITC) patent infringement case in 2006/2007 between Hewlett Packard and Acer on behalf of HP. I provided reverse engineering and technical product testing services, prepared an expert report based on my empirical findings and was subsequently deposed. Investigation No. 337-TA-606.

b. I performed failure analyses on sample products, prepared an expert report, was deposed, and testified before a jury in a 2012 LED lighting product liability case between Clutch City Sports and Entertainment (Plaintiff) and iLight Technologies et al (Defendants) Cause 2009-76645.

c. I was deposed in support of an IPR instituted by USPTO PTAB in 2018 where I represented the patent owner. (Case IPR2017-001889 Sprint Spectrum v. General Access Solutions)

d. I was also deposed in an active patent infringement case involving Bluetooth Low Energy technology, Proxense LLC v. Target Corporation, Civil Action No.: 6:20-cv-879.

B. Documents Reviewed

7. I have reviewed the Complaint in this matter, deposition testimony, documents produced in this action, publicly available documents, and Gwen Mandel's expert report. I have also had conversations with and reviewed technical documentation provided by Stan Hamilton of Rebotix Repair LLC regarding the past S/Si and current Xi EndoWrist repair

investigations. A list of the materials I have reviewed is attached as Exhibit 1. If I become aware of new information, I may modify the information in this report or supplement my opinions.

C. Compensation

8. I am being compensated for my time in this matter at the rate of $300 per hour. My compensation in this matter is not contingent on the content of my testimony or any outcome in this litigation.

II. BACKGROUND

9. I am aware that Intuitive Surgical manufactures da Vinci surgical robots and EndoWrist instruments. The EndoWrist instruments are designed to be attached to the da Vinci surgical robot, and include a use counter. There are different models and generations of the da Vinci robot. The relevant models for my analysis are the third generation robots S/Si robots and the fourth generation X/Xi robots. Intuitive developed a set of EndoWrists for each robot. The instruments developed for the Xi da Vinci robot also function with the X robot.[1]

10. The use counter is incorporated in a chip on each EndoWrist. Intuitive designed the usage counter such that it decrements one use when an EndoWrist instrument is used in surgery.[2] The actual usage counter is solely designed to track the number of times an instrument has been used in surgery and report the usage count to the robot to display the number of uses remaining on the instrument.[3]

[1] The Intuitive website describes the da Vinci X as having "the same arm architecture as the da Vinci Xi so that [the customer] can use the latest instruments" https://www.intuitive.com/en-us/products-and-services/da-vinci/systems##.

[2] McGrogan Deposition at 17:13 – 18:6.

[3] Intuitive-00512349, Intuitive-00552746.

11. It is my understanding that Rebotix Repair LLC currently repairs S/Si EndoWrists but does not currently repair X/Xi EndoWrists.[4]

A. Da Vinci S/Si EndoWrists

12. On a da Vinci S/Si EndoWrist, the use counter is programmed into a Dallas chip hard-wired to the Gen 3 S/Si instrument. Specifically, a Dallas Semiconductor (DS) DS2505 16Kb Add-Only Memory chip is used in the S/Si EndoWrists.[5] The DS2505 has three main data components: a 64-bit lasered ROM, a 16384-bit EPROM Data Memory and a 704 bit EPROM Status Memory.[6] The S and Si instruments communicate with the EndoWrist via a one wire memory bus.[7] The DS2505 memory bus stores the usage count data for the S and Si instruments. When the S/Si EndoWrist is connected to the da Vinci robot, the robot reads the data on the usage counter through a hard-wire connection to determine how many uses remain on the counter. If the da Vinci robot reads that the EndoWrist has a use remaining, it will allow that EndoWrist to be used in surgery.

13. The primary difference between the EndoWrist usage counter on the da Vinci S/Si EndoWrist and the da Vinci Xi EndoWrist is the manner in which the usage counter is accessed by the da Vinci system. For the S/Si instruments, the da Vinci system reads the data on the usage counter via a hard-wire connection, and for the Xi instruments, the da Vinci robot reads the data on the usage counter via an RFID counter.[8]

[4] Hamilton Deposition at 57:5-19, 230:22-25.

[5] Interview with Stan Hamilton.

[6] DS2505 Datasheet at 2.

[7] Hamilton Deposition at 143:12 – 144:7.

[8] McGrogan Deposition at 77:12-23.

B. General Overview of RFID Systems

14. An RFID system is a method by which data is communicated between two sources.[9]

15. A RFID system consists of two components: tags and readers. A reader is a device that includes antennas that can emit and receive RF signals from a tag and optionally power a passive RFID tag. The tag uses RF signals to communicate information to a reader.[10]

16. Unlike a hardwire connection, the RFID tag can transmit data without physically being connected to the RFID reader.[11]

17. There are two types of tags—passive and active.[12] A passive tag is powered by the signal emitted from the reader.[13] An active tag is powered by a battery.[14] Each tag can store a range of information, from a single serial number to multiple pages of data.[15]

18. An RF system for transmitting data does not affect the underlying stored data—it is a communication method for such data rather than a data storage system.

C. The Atmel CryptoRF Family on the Da Vinci X/Xi System

19. According to Intuitive's user manuals for the da Vinci X and Xi systems, each system uses RFID communication to detect installed instruments.[16] The RFID

[9] https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification.

[10] https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid.

[11] https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification.

[12] https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification.

[13] https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid.

[14] https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid, https://www.rfidjournal.com/faq/whats-the-difference-between-passive-and-active-tags.

[15] https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid.

[16] Intuitive Surgical da Vinci Xi System User Manual at E-16, "RFID communication is used by the da Vinci Xi system to detect and identify instruments and endoscopes that are installed on the system." Intuitive Surgical

communication between the X/Xi robot and Xi EndoWrists operates at 13.56 MHz and complies with ISO/IEC 14443 Type B.[17]

20. The RFID system on the X/Xi system includes an Atmel CryptoRF interface with Atmel CryptoMemory security features. I have reviewed the CryptoRF EEPROM Memory Full Specification datasheet.[18] By default the CryptoRF has no enabled security, and operates as a simple RFID EEPROM memory.[19]

21. The CryptoRF family has several security measures that can be implemented by the customer, including communications security for each User Zone, transport security, and password security. Briefly, the customer/user can opt for one of three communication security modes, namely, the default or "Normal" CryptoRF security mode which is no encryption whatsoever, the "Authentication Communication Security" mode which provides for password encryption only, and "Encryption Communication Security" mode which encrypts both passwords and user data.[20]

22. Based on my review of the Intuitive X and Xi user manuals, each system conducts a mutual authentication using a pre-shared key and the data transmitted between the da Vinci and the RFID tag is encrypted using a Secure Hash Algorithm.[21]

---

da Vinci X System User Manual at E-11: "RFID communication is used by the system to detect and identify instruments and endoscopes that are installed on the system.".

[17] Intuitive Surgical da Vinci Xi System User Manual at E-17, Intuitive Surgical da Vinci X System User Manual at E-17.

[18] Atmel CryptoRF EEPROM Memory Full Specification

[19] Atmel CryptoRF EEPROM Memory Full Specification at 117.

[20] Atmel CryptoRF EEPROM Memory Full Specification at Appendix I – K.

[21] Intuitive Surgical da Vinci Xi System User Manual at E-17, Intuitive Surgical da Vinci X System User Manual at E-17.

23. Intuitive's own cybersecurity documentation indicates that "Communications between the RFID reader and tag are encrypted."[22] Intuitive also states that the "[d]ata on RFID tag are encrypted and password-protected," and that the "[e]ncyption key and use counting data areas on RFID tag are one-time programmable and cannot be modified once written."[23]

24. According to technical documentation from Intuitive, the Intuitive Surgical Xi system (IS4000) RFID encryption is based on the SHA-1 encryption.[24] This is a dated Secure Hash Algorithm standard that has been superseded by SHA-2 and SHA-3 and is no longer recommended for use due known cryptographic weaknesses. Although SHA-1 encryption remains non-trivial to break, it is notable that according to industry sources (ComputerWorld) in 2017, "Starting with version 56, released this month, Google Chrome will mark all SHA-1-signed HTTPS certificates as unsafe. Other major browser vendors plan to do the same."[25]

25. I have reviewed Gwen Mandel's work with the Atmel CryptoRF chip and her methodology of examining the security present on the chip. Based on Ms. Mandel's work and the CryptoRF datasheet, the CryptoRF encryption communication mode applies only to the encryption of data transferred, i.e. communicated, between the Atmel RFID chip and the X/Xi robot. Neither Authentication Communication nor Encryption Communication modes are active when the chip is idled and not communicating with a da Vinci X/Xi robot.[26]

[22] Intuitive-00506542.

[23] Intuitive-00506542.

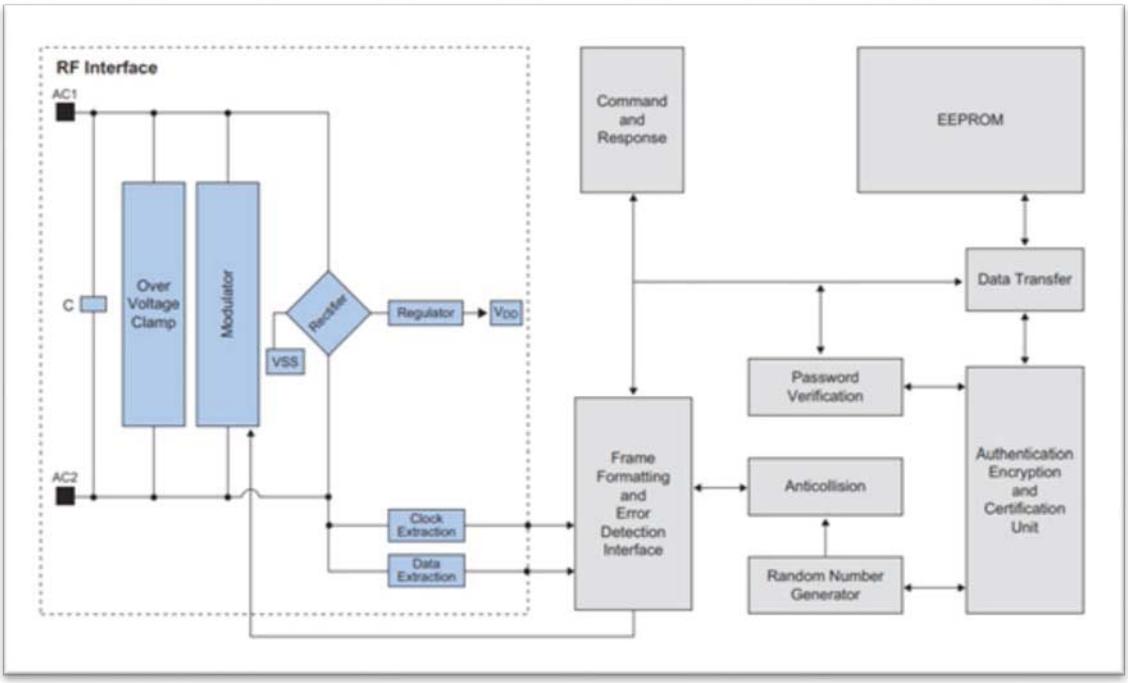
[24] Intuitive: IS4000 8mm Base Instruments Final Design Review (FDR) Slide 192.

[25] ComputerWorld "The SHA1 hash function is now completely unsafe", https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html.

[26] Atmel CryptoRF EEPROM Memory Full Specification at Appendix I – K.

26. The Atmel CryptoRF chip consists of an RFID section/portion that is responsible for communicating via an RF link, and a separate section that contains all of the data that can be communicated via the RF link.[27]

27. The user data stored in the Atmel RFID chip can be optionally access and password protected but there is no provision for encrypting stored data internal to the EEPROM block. As previously stated, the only encryption capability available on the CryptoRF chip is during password transmission (through the Authentication Communication setting) and password/user data transmission (through the Encryption Communication mode).[28] The CyrptoRF block diagram below supports this understanding as all data transferred in and out of the EEPROM block occurs via the data transfer block which is intermediary to the Authentication Encryption and Certification block.[29]



[27] Mandel Report at ¶¶ 9-14.

[28] Atmel CryptoRF EEPROM Memory Full Specification at Appendix I.

[29] Atmel CryptoRF EEPROM Memory Full Specification Fig. 1-1.

28. This comports with both Intuitive's description of the RFID security used by the X/Xi EndoWrists and my understanding of RFID security.

29. Based on my work with RFID technology and my familiarity with the Atmel CryptoRF chip, these security approaches only become active when the chip actually communicates with the robot. The EndoWrist CryptoRF chips are powered by the X/Xi robot reader through the chip's RF interface.[30] The CryptoRF datasheet states that the Authentication Communication and Encryption Communication modes remain in the designated security mode once active "until a security error occurs, a new Verify Crypto command is received, **RF power is removed**, or a DESELECT command or IDLE command is received."[31] (emphasis added). This means that the Atmel CryptoRF chip is unencrypted at rest.

30. Further, the chip can be easily removed from Xi EndoWrists for analysis.[32] Ms. Mandel was given ten chips from different models of EndoWrists that had been removed by Rebotix.[33]

D. Rebotix Repair LLC's da Vinci S/Si Repairs

31. It is my understanding that Rebotix Repair developed a method for resetting the usage counter on the da Vinci S/Si instruments. That process involves installing a small component on the EndoWrist called an Interceptor device.[34]

32. The Interceptor device allows Rebotix to reset the usage counter on individual EndoWrist instruments to its original number of uses.[35] When attached to the da Vinci

[30] Atmel Crytpo RF EEPROM Memory Full Specification at 6 ("The RF interface powers the other circuits, no battery is required.")

[31] Atmel CryptoRF EEPROM Memory Full Specification at Appendix J-K.

[32] Interview with Stan Hamilton.

[33] Mandel Report at ¶ 17.

[34] Hamilton depo tr. 143:12-25.

[35] Hamilton depo tr. 143:12-25.

S/Si robot, the robot recognizes the instrument that has been repaired by Rebotix utilizing the Interceptor device and reads the number of uses remaining based on the reset use counter.

33. My understanding of the Rebotix Interceptor device development for the S/Si robot is based on my discussions with Rebotix engineers and review of relevant Rebotix technical documentation. In short, Rebotix developed the Interceptor device by:

a. Monitoring the communications between the DS2505 memory chip on the EndoWrist and the S/Si robot.

b. Analyzing changes in the DS2505 memory contents following many iterative operations using a variety of EndoWrist instruments. Analyzing the communications between the EndoWrist instruments and the S/Si robot provided Rebotix with essential information as to the format and nature of information being communicated between the EndoWrist and the robot.

c. Performing and comparing DS2505 memory "dumps" prior to and following each EndoWrist operation allowed Rebotix engineers to map the DS2505 memory and identify the location where the use count was stored. An exemplary DS2505 memory map showing the location i.e. memory addresses, of the stored use counts, is included below for reference:

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
LASER ROM																
Dedicated location	DS2505 8-byte Serial Number															
16Kbit USER MEMORY																
	0x0	**0x1**	**0x2**	**0x3**	**0x4**	**0x5**	**0x6**	**0x7**	**0x8**	**0x9**	**0xA**	**0xB**	**0xC**	**0xD**	**0xE**	**0xF**
0000-0070	Copyright info															
0080	Copyright info cont'd					DS2505 Unique ID										0x02
0090																
00A0	EW Serial Number							Type Verify								
00B0				Ser # Verify												
0C0-150																
0160	EndoWrist Device Type															
0170	EndoWrist Device Type (cont'd)															
0180	**Available Use Count (bitwise strike counter of remaining uses – MSB at address 0180 is last use)**															
0190	**Available Use Count (cont'd)**															

d. comparison of the pre- and post- activity dumps in conjunction with communication information gathered from the 1-wire "sniffer" was used to correlate the data changes to specific activities and operations of the instrument including use count. Rebotix identified the portion of the data image that dealt with the usage counter. These reported techniques and results are consistent with conventional reverse engineering and forensic engineering methods that I have used throughout my career.

e. the extracted data and memory map of the S/Si instrument usage counter allowed Rebotix to develop a separate interface chip that would fulfill the same functions of the usage counter. As part of this process, Rebotix developed an understanding of the image on the S/Si usage counter chip and the manner in which the usage counter was coded into the memory of that chip.

34. The use of a bit-wise strike counter on the S/Si usage counter means that the uses on the S/Si counter could not be re-written/reset. A bit-wise strike counter does not allow values to be reset once the bits are struck. Moreover, according to Intuitive, the S/Si EndoWrist

included a security feature that "wiped" the ISI key used on the DS2505 chip once the use counter reached zero. According to Intuitive, "In comparison on IS3000 [S/Si robot] - ISI Key generated from Dallas unique id - key is needed for system to access Dallas data. When instrument is expired, key is wiped. All bits on dallas can only be 'cleared,' so once lives ticked off, cannot be reset."[36] This necessitated development of the Interceptor module and limited repairs to EndoWrists that had at least one use remaining.

35. Based on my conversations with Mr. Hamilton and the deposition transcripts I have reviewed, Rebotix's Interceptor chip does not affect the communication between the S/Si EndoWrists and the S/Si da Vinci surgical robots. Hospitals report no issues using the S/Si EndoWrists repaired by Rebotix in surgery.[37]

E. Status of X/Xi Repairs

36. I understand that Rebotix initially performed a brief investigation of the X/Xi usage counter in 2019, but did not invest significant time or resources into that investigation due to Intuitive's reaction to Rebotix's services for the S/Si EndoWrist instruments.[38]

37. Since seeking relief from Intuitive's conduct, Rebotix has investigated the feasibility of resetting the usage counter on the Xi instruments.[39]

38. I understand that Rebotix has identified two separate ways to extract an image file containing the use counter from the Xi EndoWrist.

[36] Intuitive: IS4000 8mm Base Instruments Final Design Review (FDR) Slide 192; Intuitive-00545094.

[37] Harrich Deposition at 34:19 – 38:1. Neither surgeons, first assists, nor scrub assists were able to discern any differences during surgery between Rebotix-repaired EndoWrists and brand new EndoWrists from Intuitive. Harrich Deposition at 38:9 – 39:3.

[38] Interview with Stan Hamilton.

[39] Interview with Stan Hamilton.

39. One method is detailed in Ms. Mandel's report. It involves using Proxmark 3 (PM3) RFID and Minicom analysis tools in conjunction with crypto libraries and publicly available key lists from CryptoRF investigators to capture and analyze data from the CryptoRF chips. Using these tools and crypto libraries allows communication with the chip and data capture from the chip. The PM3 tool is described by Proxmark as "the tool behind all major RFID Security Research breakthroughs: Mifare Classic Crypto cracking, Mifare PRNG analysis, VingCard exploitation & defeat to name a few."[40] The Minicom tool is a Linux-based serial port emulator that connects devices through serial ports and facilitates the analysis of the captured data.[41] Based on Ms. Mandel's report, her investigation has revealed four features about the CryptoRF chip

a. The CryptoRF chip does not exhibit any cybersecurity that would prevent writing data to the chip as -adpu commands have been successfully used to bypass authentication.[42]

b. Initial and follow-up scans have provided no indication that encryption of the EEPROM data at rest is implemented on all sectors of the chip or that unique passwords and keys have been implemented throughout the chip.[43]

c. Cleartext data has been extracted from the chip.[44]

d. The image on the chip can be edited and rewritten via an RF link.[45]

[40] Proxmark website, https://proxmark.com/.

[41] "Getting Started With Minicom", https://wiki.emacinc.com/wiki/Getting_Started_With_Minicom?gclid=Cj0KCQjw9O6HBhCrARIsADx5qCRdMmNHBNmxMzzPpeC2rsk0rLMkWdEQq1gCFDXfUqN_kS5t21Z9Tx0aAt9DEALw_wcB.

[42] Mandel Report at ¶ 20.

[43] Mandel Report at ¶ 20.

[44] Mandel Report at ¶ 23.

[45] Mandel Report at ¶ 27.

40. These methods are consistent with my experience in conventional RFID tag reverse engineering techniques and are capable of successfully extracting a full image of the CryptoRF EEPROM contents.[46]

41. A second independent path to obtain a full image of the CryptoRF EEPROM is by using a conventional hardware extraction or "dump" of the EEPROM by micro-soldering leads onto the external pins or internal pads of EEPROM block on the chip. This memory "dumping" approach allows direct access to the memory and its contents, bypassing the RF interface, encryption and password engines and other peripheral circuitry. In my experience, this form of conventional hardware extraction is often used when a memory source is otherwise inaccessible. Many EEPROM memories includes a conventional I2C interface because of its 2-wire simplicity, flexibility and adaptability.[47] Because the Atmel CryptoRF EEPROM chip has a conventional 2-wire I2C interface, Rebotix can micro-solder leads to the pads, bypass the RF interface and extract the EEPROM contents. Extracting those EEPROM contents should also produce a clean image file.

42. As detailed in Section 2. D. above, once Rebotix successfully extracted images from the S/Si EndoWrist usage counter, it analyzed those images to locate the usage counter, and then implemented its Interceptor process on the S/Si EndoWrist.

43. The process Rebotix has identified for the Xi EndoWrist usage counter reset is similar to the S/Si EndoWrist process: extracting images, analyzing those images to locate the

[46] For example, "The Proxmark III (PM3) is the defacto RFID research tool. There are other alternative tools but none have the community and prevalence of the PM3. It's capable of reading, writing, and emulating many of the currently available RFID tags. In addition, there is a quiet community forum where some highly-technical volunteers share custom Proxmark firmwares and much needed information about RFID research." "RFID Hacking with The Proxmark 3", K. Chung, 2017 at https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/ .

[47] "Advantages and Limitations of I2C Communication", Total Phase, https://www.totalphase.com/blog/2016/08/advantages-limitations-i2c-communication/ .

counter, and then implementing a process to reset the Xi usage counter.[48] The process Rebotix is investigating for the Xi EndoWrist usage counter reset should be significantly simpler in that the Xi EndoWrist should not require a CPLD interface device to substitute and bit mask data read from the CryptoRF device or reformat the data to satisfy the X/Xi robot. The CryptoRF chip is reprogrammable unlike the DS2505 which is an add-only memory whose contents cannot be overwritten.[49] Successful extraction and analysis of clean images from the CryptoRF EEPROM facilitates straightforward editing/rewriting of the use count and reprogramming an existing X/Xi EndoWrist CryptoRF EEPROM or replacing the existing CryptoRF EEPROM with a new, CryptoRF EEPROM personalized with the edited image file.[50]

III. OPINIONS

A. Summary of Opinions

44. I have formed three primary opinions after my review of the available information.

45. First, an image will be extracted from the Atmel CryptoRF chip on the X/Xi EndoWrists by Rebotix. The lack of security on the memory portion of the Atmel chip makes the extraction of the image from the chip's memory a simple process. I discuss two methods, an RFID software extraction method and a direct hardwire extraction method, both of which should result in successful image extraction.

46. Second, based on Rebotix's past work with the S/Si EndoWrists and its understanding of the function of the usage counter, it will identify the usage counter in the extracted image. From the initial data pulled from the X/Xi Atmel CryptoRF chip, the memory

[48] Interview with Stan Hamilton.

[49] DS2505 Datasheet at 2.

[50] Interview with Stan Hamilton.

contents on that chip appears to be virtually identical to the S/Si usage counter. Creating a memory map of the X/Xi usage counter after image extraction would result in an understanding of where the usage counter is and how to reset it.

47. Third, Rebotix will have the capability to implement a reset of the usage counter on the X/Xi EndoWrists. After image extraction, the process of resetting the usage counter on the X/Xi EndoWrists will be easier than resetting the usage counter on the S/Si EndoWrists due to the reprogrammable nature of the CryptoRF chip. This means that the implementation of the Interceptor process would not need to circumvent that bit-wise strike counter, and instead could directly alter the image on the CryptoRF chip to reset the use counter to its original value. Additionally, the X/Xi usage counter is also contained on a chip that can be easily removed from the X/Xi EndoWrist and replaced once with a new CryptoRF chip that can subsequently be reprogrammed multiple times.

B. An image will be extracted from the Atmel CryptoRF chip on the X/Xi EndoWrists by Rebotix

i. Overview of image extraction

48. Image extraction refers to taking an image contained on a chip's memory and transferring it to a computer or other reader in readable form.

49. An extracted image provides full information about what is stored on the chip, the manner in which the chip's memory is organized, and how the functions that can be performed by the chip operate.

ii. Process of image extraction

50. Several security methods can make the extraction of an image from the memory of a chip more difficult. First, if the data on the chip itself is encrypted, the image extracted from the chip would first need to be decrypted before being readable. Second, hardware security

could be implemented on the chip to prevent external hardware connections from attempting to extract data. Third, physical anti-tampering mechanisms can be employed to make reverse engineering efforts such as dying, scanning probes, and voltage contrast methods more difficult to implement.[51]

51. By contrast, if there are no security methods implemented on the actual memory portion of the chip, extracting a full image is straightforward, and can be accomplished using multiple different methods depending on how the chip communicates.

52. If a chip communicates via a hardwire connection and has no additional security, an image can be extracted from the chip's memory using a simple hardwire connection. A hardwire connection to the chip's external pins or internal pads allows for the chip's memory contents to be read directly.[52]

53.. If a chip communicates using an RFID link, the same hardwire connection method is possible. For the Atmel CryptoRF chip, where the section of the chip responsible for communicating data via an RF link is separate from the memory that contains the data to be transferred, this hard-wire connection involves a direct connection to the EEPROM memory. And none of the security measures that I identified above appear to be in use or active to secure that EEPROM memory.

iii. Extraction from the Atmel CryptoRF chip on the da Vinci Xi EndoWrists

54. As discussed above, the Atmel CryptoRF chip used on the da Vinci Xi EndoWrist does not have active security implemented on the memory portion of the chip that

[51] "Use an External Encrypted EEPROM to Secure Data in Embedded Systems" Digi-Key, https://www.digikey.com/en/articles/use-external-encrypted-eeprom--secure-data-embedded-systems.

[52] Extended Learning Institute (ELI) at Northern Virginia Community College (NOVA). "Introduction to Computer Applications and Concepts." *Lumen*, courses.lumenlearning.com/zeliite115/chapter/reading-read-only-memory/.

stores the image. The only implemented security activates when the RFID portion of the Atmel CryptoRF chip communicates with the da Vinci robot.

55. Rebotix has investigated two methods for extracting the image from the Atmel CryptoRF chip. One method operates via an RFID connection to the chip. The other operates through a hard-wire connection to the EEPROM memory on the CryptoRF chip.

iv. RFID Method

56. The methodology described by Ms. Mandel in her report resulted in a connection to the Atmel CryptoRF chip, the establishment of bi-directional communication, and the transmission of data from the Atmel chip to the reader.

57. The data retrieved from the chip by Ms. Mandel was not in any way encrypted or otherwise secured. This is what is referred to as "clear data." A chip's image consists of the clear data with a particular organization.

58. Because the connection with the chip has resulted in the communication of clear data, the full unencrypted image can be extracted from the chip. The communication of clear data means that any security on the communication and any security on the actual data itself has been overcome. When data extraction methods result in clear data being extracted, the only step that remains before full image extraction is some additional time. An unencrypted (clear text) binary image file is readily convertible to usable, editable text using a standard hex editor.[53]

v. Hard Wire Method

59. In parallel to Ms. Mandel's method, it is my understanding that Rebotix is extracting the image from the Atmel CryptoRF chip using a hard wire connection to the actual

[53] 010 Editor Manual - Using the Hex Editor, www.sweetscape.com/010editor/manual/UsingHexEditor.htm.

EEPROM memory in the chip.[54] This method bypasses any RFID link entirely and allows for direct access to the memory image.

60. This method is commonly used in the data security and extraction field to retrieve data directly from memory devices.[55]

61. With a direct hardwire connection, if there are no physical anti-tampering security measures, full image extraction occurs over the direct connection to the chip's memory. And here, there are no security measures on the chip's memory that inhibit a hardwire extraction.[56]

C. The usage counter in the extracted image will be identified by Rebotix

i. Analyzing an extracted image

62. After an image is extracted from a memory device, that image is analyzed to determine how it is structured. In my experience as a reverse engineer, this process of image analysis is simple as long as the underlying image does not have additional encryption.

63. The generally accepted steps to perform a binary image analysis involve using a binary image scanning tool such as binwalk and an open-source binary file scanner. Using those two tools in conjunction with a hex editor, binary data is converted into individual files and the overall file structure and organization of an image is established. This process converts a binary image into readable, editable files.[57]

64. Every conventional digital memory is a device that stores bits (i.e. 1's and 0's) in an organized fashion. A full binary image of the memory includes all of the individual bits

[54] Interview with Stan Hamilton

[55] Fukami, Aya, et al. "A New Model for Forensic Data Extraction from Encrypted Mobile Devices." *Forensic Science International: Digital Investigation*, Elsevier, 27 May 2021, www.sciencedirect.com/science/article/pii/S2666281721000779.

[56] Atmel CryptoRF EEPROM Memory Full Specification at 35.

[57] Canonical. *Ubuntu Manpage: Binwalk - Binary Image Search Tool*, manpages.ubuntu.com/manpages/trusty/man1/binwalk.1.html.

that are stored in the memory. Binary analysis then organizes or structures those bits into recognizable groups that represent individual files. Once those bits are organized, then the files can be read, their functions identified, and their values edited. This structural analysis provides an understanding of how the memory on the chip is programmed and how the chip fulfills its required function. All of a memory device's information is necessarily contained in that image.

ii. The extracted image from the Atmel CryptoRF chip

65. The image on the Atmel CryptoRF chip on the da Vinci EndoWrist fulfills two primary required functions. First, the image contains information that identifies the model of EndoWrist.[58] Second, the image contains the use counter and the number of remaining uses on the use counter.

66. The Atmel AT88SC6416 CryptoRF RFID chip contains 8,192 bytes of User Memory equally divided into 16 user zones of 512 bytes each.[59] Ms. Mandel has analyzed the data contained in each User Zone and determined that User Zone 1 contains the use counter and other relevant information about the Xi EndoWrist.[60] This allows Rebotix to focus only on the User Zone data from User Zone 1 to determine which data in that zone need to be edited in order to produce an image file consistent with the original number of uses on the use counter.

iii. Ms. Mandel's investigation has identified the location of the usage counter

67. Ms. Mandel describes an analysis of the User Zones on the Atmel CryptoRF chip.[61] In that analysis, Ms. Mandel identified the User Zone that contains relevant information

[58] Intuitive Surgical da Vinci Xi System User Manual at E-16, "RFID communication is used by the da Vinci Xi system to detect and identify instruments and endoscopes that are installed on the system."

[59] Atmel CryptoRF EEPROM Memory Full Specification, Tables 3-1 and C-6.

[60] Mandel Report at ¶ 17.

[61] Mandel Report at ¶ 17.

about the model of the EndoWrist and its serial number.[62] Further, Ms. Mandel identified the User Zone that contains the relevant information about the usage counter.[63]

68. Ms. Mandel's ability to identify these specific pieces of information in the image demonstrates that the precise location of the usage counter on the image can be readily identified. And because Ms. Mandel has already narrowed the location of the use counter to a particular User Zone, Rebotix can isolate the use counter function on that zone.

iv. Several additional factors make the process of Rebotix's image analysis for the Xi EndoWrist CryptoRF chip easier than others that I have encountered in my career

69. Generally, in my experience, when a reverse engineer encounters an image for the first time, that engineer will not have prior experience with that image.

70. Prior experience with similar images and functions of similar chips makes the process of image analysis easier.

71. If two chips have similar or identical images, prior analysis of the image of the first of the two chips (Chip A) makes the analysis of the second chip (Chip B) simpler. Even if the initial analysis of Chip A takes significant time and resources, image analysis on Chip B can use the foundational understanding of Chip A's image.

72. Further, if two chips fulfill similar or identical functions, understanding the manner in which one function is implemented in a chip's image provides an understanding of how that function is implemented in another chip's image, even if there are differences between the images themselves.

[62] Mandel Report at ¶ 17.

[63] Mandel Report at ¶ 17.

73. Rebotix already created a memory map of the S/Si EndoWrist usage counter when it developed the Interceptor process for the S/Si EndoWrist.[64] This gave Rebotix an understanding of the memory structure, how data pulled from the chip is organized, and what portions of the S/Si chip's memory contained the usage counter.[65]

74. This work established both a direct understanding of the image and an understanding of how the usage counter function was implemented on that chip's memory architecture.

75. The Atmel CryptoRF chip has significant functional similarity, because it implements the same usage counter function as the S/Si. The chip decreases the number of available uses by one after an Xi EndoWrist is used in surgery.[66] An understanding of how that function was implemented in the S/Si EndoWrist usage counter makes understanding that implementation in the Xi image simpler.

76. Moreover, the data retrieved by Ms. Mandel from the Atmel CryptoRF chip on the Xi EndoWrist is highly similar or identical to the data that Rebotix extracted from the Dallas chip on the S/Si EndoWrists.[67] This similarity between the data extracted from the Xi EndoWrist and prior data analyzed by Rebotix on the S/Si EndoWrist makes image analysis a straightforward process.

[64] Interview with Stan Hamilton.

[65] Interview with Stan Hamilton.

[66] McGrogan Deposition at 78:10-18.

[67] Interview with Stan Hamilton.

D. Rebotix can use the extracted image to reset the usage counter on da Vinci Xi EndoWrists

77. In my professional experience, once an image has been extracted from an EEPROM chip, analyzed, and converted to a hexadecimal file, an EEPROM programmer can use that hex file to reprogram the existing EEPROM or program a new replacement EEPROM. This general process of extraction and reprogramming is a basic methodology that has been successfully used in the reverse engineering of commercial EEPROM memories for many years.[68]

i. There are two approaches to reset the usage counter on the Xi EndoWrist

78. The first is to utilize Ms. Mandel's method of establishing an RFID connection with the appropriate authentication and keys and writing new values to the User Zone.

79. The second is to modify the extracted image, return the use counter to its original state, write that image to a new Atmel CryptoRF chip, and replace the original chip on the Xi EndoWrist with the new chip.

ii. RFID Connection Writing

80. Ms. Mandel's methodology was successful in issuing 14a and 14b commands to the Atmel CryptoRF chip. Ms. Mandel also successfully established a direct connection with the User Zone section of the memory image and both sent data to and received data from that User Zone.

81. With the extracted image identified and organized, sent data can modify that portion of the image that contains the remaining value on the usage counter.

[68] Conti, Gregory, et al. "Visual Reverse Engineering of Binary and Data Files." *Visualization for Computer Security Lecture Notes in Computer Science*, Sept. 2008, pp. 1–17., doi:10.1007/978-3-540-85933-8_1.

82. Intuitive's description of the use counting data areas being one-time programmable and unable to be modified once written do not change my conclusion.[69] Ms. Mandel was able to access the User Zone and establish direct read/write command communication.

83. The actual modification of the count set on the usage counter does not require a new write of an entire image to the usage counter. Instead, it merely requires the remaining value of the usage counter to be adjusted. Ms. Mandel's analysis of the CryptoRF User Memory has further confirmed that the stored code is small and confined to a single user zone. The use counter value on that user zone consists of only a few bits of data specifying the remaining uses. There are multiple reasons that the portion of the use counter that stores the number of uses is modifiable via an RFID connection.

84. First, the actual value remaining on the use counter has to be changed after being used in surgery. When the da Vinci X or Xi robot establishes a connection with the robot, it reads the value on the usage counter.[70] And it must also be able to cause that usage counter value to change after it is used in surgery.[71] Because the value of the usage counter is variable by the very nature of its function, that value is capable of being changed.

85. Second, Ms. Mandel's method indicates that once the appropriate connection with the Atmel CryptoRF chip is established, read/write commands can be freely issued to and are received by the chip.[72] Those commands include hex commands, and commands to alter data present on the chip.[73] Based on my review of Ms. Mandel's report and her ability to have

[69] Intuitive-00506542.

[70] Intuitive-00552746; Intuitive-00593473.

[71] Intuitive-00593477- Intuitive-00593478.

[72] Mandel Report at ¶¶ 25-26.

[73] Mandel Report at ¶¶ 26-27.

those commands issued and received, there is no barrier to writing new values to the usage counter on the chip once an RF connection is successfully established.

86. Third, there is no additional encryption or security barrier that prevents writing new data to the chip. As discussed previously, the extraction of clear data from the chip once an RFID connection has been established indicates that there are no additional barriers to writing data. As discussed previously, the data stored in the CryptoRF EEPROM memory is not encrypted and there are no additional physical security features on the chip to prevent extraction of a clean image file.

87. Fourth, the encryption keys are "behind" the security fuses and will also be directly extracted as part of the EEPROM image file and therefore accessible to Rebotix. The CryptoRF datasheet states that "These [security] fuses do not control access to the user memory; user memory access rights are defined in the Access Registers. The security fuses are used to lock the state of the Access Registers, Passwords, Keys, and other configuration data during the personalization process so that they cannot be changed after a card is issued." Since the use counter data by definition must be allowed to change as a function of EndoWrist use, it cannot be a value locked by a security fuse.

iii. Hardware Chip Replacement

88. A second approach to resetting the usage counter involves adjusting the usage counter value on the extracted image, copying that image to a new blank Atmel CryptoRF chip, and installing that Atmel CryptoRF chip back into the Xi EndoWrist.

89. Based on Ms. Mandel's report, the Atmel CryptoRF chips have some specific identifying information (such as serial numbers and model of EndoWrist), but the remaining image is identical.

90. Adjusting the image after it has been extracted to reset the usage counter involves altering the bits of data that specify the current use counter value and returning them to their original number of uses. The original EndoWrist device has a published specification on the initial value of the usage counter.[74] Adjusting the image would involve modifying the bits of data to correspond to the original published specification for the number of uses.

91. After the image is adjusted to reset the usage counter to its original value, that image can be written to a blank Atmel CryptoRF chip. The image would be identical to an original Atmel CryptoRF chip included on the Xi EndoWrist, with a reset number of uses to the original use count. And because EndoWrists function regularly with a use counter showing that original value, the new chip would cause the repaired EndoWrist to function just as a brand new EndoWrist would.

92. Nothing about the image or the general structure of the Atmel CryptoRF chip precludes this type of image rewrite to a new chip. And the design of the Xi EndoWrist does not preclude removing the Atmel CryptoRF chip and installing a new chip containing the new image. In fact, due to the inherent reprogrammable nature of the CryptoRF chips, the chip replacement repair process should only be necessary once, allowing for the X/Xi EndoWrist to repaired multiple times without further chip replacement.[75]

IV. OTHER ISSUES

A. Intuitive's own security testing

93. Based on documentation from Intuitive, it appears that Intuitive engaged a third party to investigate potential security issues with the RFID system used on the da Vinci

[74] Intuitive-00671027; Intuitive-00671034.

[75] Interview with Stan Hamilton.

X/Xi.[76] In that report, prepared in November of 2013, the third party conducted testing on the RFID system using a standard RFID reader/writer programming device.[77] As part of that testing, the third party performed a number of test cases, including test cases to "spoof daVinci attachments," "to tamper daVinci attachments metadata," and "attempt reading sensitive data being passed from the attachment to the daVinci system."[78] At that time, the third party concluded that "[n]o observable software faults or security issues were discovered during RFID testing."[79]

94. This outdated report does not change my opinion for four reasons.

95. First, the methods and technology used to test the RFID interface was an extremely simple device setup using severely outdated technology. The report describes the custom testing harness used to perform tests as a "MIFARE and NFC capable RFID reader/writer."[80] This setup is a simple RFID reader that is designed to only interface or write to devices that have no active RFID security measures. Because the Atmel CryptoRF includes security that becomes active when a direct RFID connection is established in this manner, it is unsurprising that a basic interface attempt with a simple RFID reader/writer, like the one used by the third-party in 2013, would be unsuccessful.

96. Second, the described tests used a flawed and outdated methodology for accessing the Atmel chip. Based on the description provided in the report, there was no initial sniffing of data transmitted by the RFID chip performed.[81] Without this initial data sniffing, there

[76] Intuitive-00506582 (Cylance Professional Services Technical Report).

[77] Intuitive-00506593 – Intuitive-00506594.

[78] Intuitive-00506594.

[79] Intuitive-00506594.

[80] Intuitive-00506593.

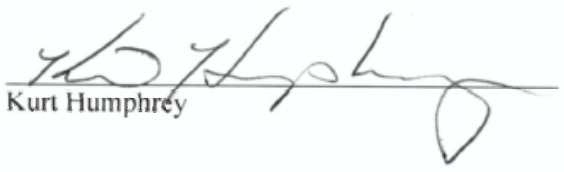
[81] Intuitive-00506593 – Intuitive-0050694.

is no way to customize the RFID connection to transmit proper authentication keys or protocols. Both Authentication Communication and Encryption Communication modes in the CryptoRF chip are "activated by performing Mutual Authentication between the host system and the PICC using the Verify Crypto command."[82] This means that the Xi robot (the host) and the CryptoRF chip (the PICC) must share encrypted passwords that a simple RFID reader could not decrypt. The method employed by Ms. Mandel used a sniffing method to monitor data being transferred before attempting to make direct reads and writes to the device.[83] This observation of initially transmitted data is an important step that allowed Ms. Mandel to establish a two-way connection with the Atmel CryptoRF chip and extract data from the chip. This was not accounted for in the third party testing conducted in 2013.

97. Third, the third-party testing did not investigate a hard wire connection to the chip for the purpose of extracting an image from the Atmel chip. The report did not discuss any security implemented on the chip that would prevent this type of hard-wire connection.

98. Fourth, the third-party testing did not investigate whether it would be possible to replace the Atmel CryptoRF chip with a different chip with a rewritten image. As discussed above, there is no implemented security method that prevents this approach from being successful.

Executed on July 26, 2021,



Kurt Humphrey

[82] Atmel Crypto RF EEPROM Memory Full Specification Datasheet Appendices J, K.

[83] Mandel Expert Report at ¶ 17.

Exhibits 1

- Interview with Stan Hamilton on 7/23/21
- June 7th, 2021, Deposition of Anthony McGrogan
- June 4th, 2021, Deposition of Stan Hamilton
- Atmel CryptoRF EEPROM Memory Full Specification
- Dallas Semiconductor DS2505 Data Sheet
- Da Vinci X Manual
- Da Vinci Xi Manual
- Intuitive-00506505-Intuitive-00506641
- Intuitive-00512348-Intuitive-00512353
- Intuitive-00544903-Intuitive-00545124
- Intuitive-00552745-Intuitive-00552759
- Intuitive-00593443-Intuitive-00593480
- Intuitive-00671020-Intuitive-00671035
- Expert Report by Gwen Mandel
- Fukami, Aya, et al. "A New Model for Forensic Data Extraction from Encrypted Mobile Devices." *Forensic Science International: Digital Investigation*, Elsevier, 27 May 2021, www.sciencedirect.com/science/article/pii/S2666281721000779.
- Conti, Gregory, et al. "Visual Reverse Engineering of Binary and Data Files." *Visualization for Computer Security Lecture Notes in Computer Science*, Sept. 2008, pp. 1–17., doi:10.1007/978-3-540-85933-8_1.

Exhibit 2

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

SURGICAL INSTRUMENT SERVICE COMPANY, INC., Plaintiffs, v. INTUITIVE SURGICAL, INC., Defendants.	Case No. 3:21-cv-03496-VC Honorable Vince Chhabria

EXPERT REPORT OF PAUL D. MARTIN, PH.D.

January 18, 2023

Highly Confidential – Subject to Protective Order

1. My name is Paul D. Martin, Ph.D. I have been retained as an expert on behalf of Defendant Intuitive Surgical, Inc., in the above captioned matter. I have been asked to submit this report covering certain technical matters at issue in the case.

I. QUALIFICATIONS

2. I am presently the Director of Firmware Security and Senior Research Scientist for Harbor Labs, Inc. I hold B.S., M.S.E., and Ph.D. degrees from Johns Hopkins University, with all degrees, including my doctorate, being in computer science. My current curriculum vitae (CV) is attached to this report as Attachment A. My education and experience in these fields are set forth in detail there. Attachment A also includes a list of publications authored in the previous 10 years and a list of all other cases in which I have testified or been deposed in the past four years.
3. I am an expert in the technical subject matter areas relevant to this report. All opinions and facts stated in this report are true and correct to the best of my knowledge. If called upon to testify, I could and would testify to the truth of the following.
4. Harbor Labs is being compensated for my time at an hourly rate of $580 per hour. My compensation and the compensation to Harbor Labs is not dependent on and has not affected the substance of my statements in this report. Neither my compensation nor that of Harbor Labs is affected by or contingent upon the ultimate outcome of this litigation, and I have no other interest in this proceeding.
5. I first started programming at the age of 14 with the C programming language. I began writing source code in C, Python, and Java shortly thereafter. I began working in the software industry in 2008, when I obtained my first independent consulting client—the

Brandeis University Hardware Repair Shop. I wrote and edited the source code to a program for their ticketing system to interface with a label printer. This enabled the computer repair shop to automatically print labels associated with tickets in order to easily identify customers' devices.

6. In 2009, I began working for a security consulting company called Independent Security Evaluators in Baltimore, Maryland. I worked on a wide variety of security and privacy projects including projects to test and break the DRM scheme of a magazine distribution application for IOS and Android (at the behest of the developer of said application), projects to test implementation code for cryptographic secret splitting, projects to assist with fuzz testing for security vulnerabilities of a variety of software applications, software development projects to automate testing of antivirus and antimalware solutions, and a variety of other security-related projects. I worked for ISE as an intern throughout the semesters and summers until August 2011. In 2010, I also designed a security architecture for a large-scale digital curation system meant to be a major inter-university initiative to create a successor to existing digital curation systems that could be used for decades.

7. In spring 2011, I completed my bachelor's in computer science at Johns Hopkins University, and I also retained an independent consulting client, the University of Michigan, for whom I performed a penetration test and security assessment of a cloud-based research system that they planned to deploy. In fall 2011, I began working towards my Ph.D. in computer science, also at Johns Hopkins University, and I began researching computer security and privacy systems in order to both design novel technologies for securing computing systems and to also bridge the interface gap between users and their technology. As such, my research focused not only on developing technical solutions to

novel security and privacy systems but also on presenting these solutions in a way that non-technical users could understand.

8. During my time as a Ph.D. student at Johns Hopkins, I co-instructed a short course called, "Introduction to Hardware Hacking," with a colleague, Dr. Michael Rushanan, which was the highest-rated course in the computer science department (based on student reviews) during the winter session in which it was offered. In this course, we offered lessons on a variety of topics including modifying game consoles and device firmware; electronics repair; binary analysis and modification; network traffic analysis; and web-based vulnerability assessment and exploitation.

9. I finished my Ph.D. by successfully defending my dissertation, entitled "Securing Medical Devices and Protecting Patient Privacy in the Technological Age of Healthcare," on February 12, 2016, at the age of 26. My doctoral thesis tells the story of a secure healthcare practice of the future in which technology is seamless to use for healthcare providers while providing a much higher standard of security than is typical today. It focuses on the juxtaposition of usability and security with an emphasis on simplicity, automation, and error-proofing of security controls.

10. During my doctorate and afterwards, I have produced, peer-reviewed, and published research in areas such as fingerprinting, anomaly detection, multifactor authentication and embedded systems security. In many of these cases, I focused not only on designing novel security systems but also on designing usable web-based security systems for controlling them and understanding their data output. In fact, some of my research has formed the basis for commercial products and services. For example, in my work on integrated audit and access control, which was funded in part by Accenture Labs, I developed a Hadoop-

based application to perform large-scale statistical analysis of audit logs from an electronic medical record system. As part of this work, I also designed a web application to automatically produce human-readable reports and graphs for use in consulting. The system I designed is able to discern implicit access models in a hospital and to then audit EMR use based on these models in order to detect potential HIPAA violations. Accenture subsequently patented this technology.

11. Similarly, in my work at Applied Communication Sciences in 2013, I designed and implemented a web-based traffic visualization dashboard and analysis system for field area smart grid networks that could be used to quickly gain an understanding of the current state of a SmartGrid network as well as to detect unexpected anomalies in the network. Applied Communication Sciences subsequently patented this work and continued to build on the project. To my knowledge, they actually sold and/or still sell this product as part of their SecureSmart Managed Security Service product offering.

12. I have worked on and published two research projects related to improving the quality and ease-of-use of authentication technologies in healthcare settings. In one project, I and my co-authors designed a cryptographic security system for wireless technology used in medical networks. The result was an indoor location tracking system consisting of unspoofable Bluetooth Low Energy beacons. These beacons were placed around a building and mapped to a backend such that a user could report which beacons he or she was within range of in order to be used as a secondary authentication mechanism for accessing patient medical records. In the way that we designed and envisioned the system, a doctor would log into a mobile device which would connect to a web-based backend. As the doctor walked past patient rooms, he or she would be automatically presented with medical

records of nearby patients. In another project, I and my co-authors designed an authentication bracelet for doctors that would receive a Kerberos ticket upon login to a modified computer terminal through use of low-energy electrical signals transmitted over the wearer's skin. When using other hospital terminals, this Kerberos ticket could be sent back over the wearer's skin to the custom contact on the terminal in order to allow the doctor to login without a password. The bracelet was also designed to immediately lose the cryptographic secret upon being removed from the user. This allowed doctors to authenticate to a computer on wheels terminal at the beginning of their shift and then to subsequently authenticate themselves in various other contexts as they went about their shift merely by touching specially designed access panels.

13. My recent research has focused primarily on embedded systems security with an emphasis on binary analysis, anomaly detection, and automated security enforcement. Some of this research has focused on reverse engineering embedded medical devices to add novel security monitoring technology onto insecure devices. This security system can be soldered directly to the CPU of the medical device in order to perform control-flow integrity for purposes of profile building and enforcement. Such techniques prevent against control-flow hijacking attacks as well as physical attacks that leverage configuration modes to change device settings. In another case, I designed a system to automatically discern name and version information from binaries on embedded devices in order to build a software profile of the platform configuration of the device, which can then be cross-referenced with a vulnerability database. I have also written a patent on this specific technique.

14. In February 2016, I joined Harbor Labs full-time as a research scientist. In January 2019, I was promoted to senior research scientist. At Harbor Labs, I manage client engagements and lead teams in the areas of security analysis and source code analysis.

15. As part of my work at Harbor Labs, I have worked on the design and implementation of cryptographic protocols for securing data in medical devices. As another part of my work, I have worked with companies to reverse engineered their medical devices to discover and exploit previously unknown vulnerabilities.

16. A substantial portion of my role at Harbor Labs is supervising source code review teams as part of legal consulting engagements. As part of this work, I have reviewed software systems of varying sizes, often totaling in the millions or billions of lines of code. I have reviewed products in the security space, television-based set top boxes, network appliances, numerous web-based enterprise systems, email management systems, telephony products, embedded system bootloaders, social network platforms, and countless other products. I have conducted and/or supervised source code reviews in more than 48 cases.

17. I am also the technical and development lead for a firmware security analysis engine for a product that we are developing called Firmware IQ. In this role I perform experiments, write source code in Python, review the source code written by others, and supervise documentation and testing efforts.

II. SCOPE OF ENGAGEMENT

18. I understand that Surgical Instrument Service Company, Inc. (hereafter SIS) contends that Intuitive Surgical, Inc. (hereafter Intuitive) has engaged in allegedly anticompetitive behavior by using cryptographic controls on EndoWrist devices.

19. I have been asked to review the report of Mr. Kurt Humphrey and to provide my opinions on the subjects he covers. I have also been asked to provide my own, independent opinions on the security concerns with respect to RFID systems, the reasons for encrypting them, and the risks associated with not doing so. I also have been asked to opine on the differences between the chips used in different generations of EndoWrists and the advantages of the RFID system over the previous generation of technology. Finally, I have been asked to opine on the differences of reverse engineering wired and wireless chips.

III. SUMMARY OF OPINIONS

20. It is my opinion that wireless systems, including the RFID system used in certain EndoWrist Instruments compatible with the X/Xi da Vinci Surgical Systems (referred to throughout as "X/Xi instruments" or "X/Xi EndoWrists"), have additional security concerns related to the wireless nature of the communication that differentiate them from wired systems. To attack a wired system, an attacker generally must have close physical proximity to the system, and the attacker is thus more susceptible to physical security controls. Unlike a wired system, a wireless system must contend with attackers that do not require direct physical access to the system, but who are either within radio range of the system or have placed equipment within range of the system. Due to these concerns, wired systems require cryptographic controls in order to provide a similar level of data security to a system with a direct physical connection.

21. It is my opinion that the encryption Intuitive employed on the X/Xi instruments is consistent with these risks and reflects best practices to protect the data contained on or transmitted through the RFID system from being intercepted or altered. The RFID chip

encryption protects not only the use counter information on the X/Xi instruments but also the tool user ID, instrument drive parameters, and calibration data for the instrument.

22. It is my opinion that the Atmel RFID chip used in the X/Xi instruments offers substantive improvements over the DS2505 chip used in previous generations of EndoWrist Instruments compatible with the S/Si da Vinci Surgical Systems (referred to throughout as "S/Si instruments" or "S/Si EndoWrists"), including increased memory, faster data access, and improved reliability and endurance.

23. Furthermore, it is my opinion that a wireless communication channel offers general improvements over a wired communication channel. Wired technology requires special care and attention in the design and manufacturing process, to prevent against accidental damage and to ensure that physical strain is minimized. In contrast, wireless technology has lower manufacturing complexity, and it has increased reliability against physical damage. This is especially useful in systems such as an EndoWrist where physical mobility has the possibility of damaging or disconnecting the wire, reducing reliable operation of the device.

24. It is my opinion that Mr. Humphrey's analysis of the encryption on a newer generation of instruments currently in the design phase (referred to throughout as "Skywalker instruments" for consistency with the Humphrey report) is substantively flawed in that it ignores the difference in a wired versus wireless communication channel in terms of a threat perspective and also does not reflect an actual product on the market, as it only evaluates an in-progress design that is unreleased to the public.

25. Finally, it is my opinion that reverse engineering the X/Xi instruments involves a different process than reverse engineering the S/Si instruments, though Mr. Humphrey's

analysis on the extent of the time and resources needed to reverse engineer the X/Xi instruments is speculative.

IV. BACKGROUND ON CYBERSECURITY AND CRYPTOGRAPHY

26. Security is the process of preventing unauthorized third-party access to protected data and privileged devices or, more generally, system functionality.

27. When considering a system's security, it is not enough to merely list all of the security controls in place. One must consider how users use the system. One must also evaluate attackers in terms of goals, capabilities, and return on investment. That may require assessing an attacker's potential motivation, whether they would require sophisticated hardware, what information would be accessible, how many users would be impacted from an attack, whether an attack would be costly, and other factors specific to a given system. The context of a system's use can greatly influence the answers to these questions as a security system in one context may be grossly insecure compared to the same system in another context. For example, a security analysis of a laptop requires an understanding of how the system is accessed, who accesses it, when and where they access it, and how and where data is stored. These details give insight into the threat model.

28. A threat model formalizes security risks to the system by enumerating vulnerabilities, weaknesses, and defects, and considers the risk of those defects if exploited by an attacker. It is industry best practice for device manufacturers to perform a formal security analysis, including a threat model, of a product before bringing it to market. A threat model formally defines attackers in terms of goals, capabilities, and relation to the system.

29. While a threat model exposes security risks, security requirements or controls address and reduce these risks. In other words, security requirements prescribe how a device should be secured to reduce the risks identified in the threat model. Typical security requirements include access controls to limit the exposure of data and functionality and the use of standardized cryptographic algorithms and protocols to protect data at rest and in transit via a network.

30. Cryptography is the study of how to hide information. It is often used to secure or protect electronic communication between entities. Cryptography includes two general methods for altering the readability of information: encryption and decryption. Encryption is the practice of converting readable information into unreadable information through use of a key; decryption is the inverse. Those skilled in the art refer to readable information as plaintext and encrypted information as ciphertext. In theory, by encrypting private data, an attacker without the decryption key will only have access to the ciphertext, which does not leak any data, thus keeping the data confidential.

V. SECURITY VULNERABILITIES OF WIRELESS SYSTEMS AND ENCRYPTION AS A MITIGATION MEASURE.

31. I understand that Intuitive has produced different generations of EndoWrist instruments over the years. These include the IS2000 and IS3000 (S/Si) instruments and IS4000 (X/Xi).[1] I understand that another IS5000 series currently is in development but not yet finalized or available for sale.[2] While the EndoWrist S/Si instruments use a direct wired connection for communication between the da Vinci Robot and the EndoWrist, the

[1] Duque Dep. Tr. ("Duque") at 23:25–24:19.
[2] Somayaji Dep. Tr. at 128:1–10.

EndoWrist X/Xi instruments use a wireless connection over an RFID interface to send identification information, instrument drive parameters, calibration, and use counts from the EndoWrist X/Xi to the da Vinci robot.[3]

32. Wired connections have different security considerations than wireless connections. Although there are numerous security considerations besides just the connection between the da Vinci Robot and EndoWrist, I limit the following discussion to security considerations with respect to this connection only, so that I can more easily compare this aspect of the system design.

33. A da Vinci Robot using a wired connection to an S/Si EndoWrist has different security concerns and a different threat model than a da Vinci Robot using a wireless connection to an X/Xi EndoWrist. The threat model with respect to the wired connection is simpler than the threat model with respect to the wireless connection.

34. An important threat consideration for a wired connection is an attacker with direct physical access to the system. In the absence of mitigation measures, an attacker with physical access can tamper with the connection between the da Vinci Robot and the S/Si instruments. For instance, a passive attacker can eavesdrop on the physical connection by tapping it, in order to observe the data sent across. An active attacker also could intercept and change the data. In both cases, the attacker generally must have close physical proximity to the da Vinci system when attacking a wired system, and is therefore more susceptible to physical security controls such as security guards and security camera monitoring.

[3] Duque 30(b)(6) Dep. Tr. ("Duque 30(b)(6)") at 20:7–21:5; Somayaji Dep. Tr. at 109:6–22.

35. That is to say, for the wired connection of the S/Si EndoWrists, the threat model would contain adversaries in the classes "passive physical attacker" and "active physical attacker."

36. In contrast to the threat model of the S/Si EndoWrists where system communications occur through a direct physical connection, the X/Xi EndoWrists use a wireless connection between the da Vinci Robot and the EndoWrist to convey via radio frequency ("RF") certain system communications, including identification information, instrument drive parameters, calibration, and use counts.[4]

37. Therefore, for the wireless system, the threat model is a superset of the threat model for the wired system. The model must be expanded to also include nearby attackers (both active and passive) within radio range. A wireless system like the radio frequency identification ("RFID") system in the X/Xi systems not only has to contend with active and passive attackers, it also needs to consider the possibility that an attacker does not have direct physical access to the da Vinci system but is either near the robot (within radio range) or has placed equipment near the robot and is thus able to perform the attack on the RF communication channel without a nearby physical presence.

38. To provide a comparison, a typical computer network may be wired, wireless, or both. In a wired network that uses CAT5-7 or fiber optic cabling, security concerns are primarily related to physical attackers. Therefore, wired network connections typically do not leverage link-layer encryption because administrators are not worried about wireless attackers eavesdropping on the connection to observe the data sent across. On the other

[4] Somayaji Dep. Tr. at 56:4–60:9.

hand, computers on wireless networks broadcast all of their data publicly in order to enable communication between the access point and the endpoint. Because all wireless networking equipment sharing a particular standard implementation (*e.g.* 802.11ac) is able to communicate with all other such equipment, an attacker can easily eavesdrop on communications between any client and a base station.

39. For this reason, encryption is used to ensure privacy and integrity of communications on wireless networks. Originally, the first widespread encryption standard for Wi-Fi networks was called WEP, which stood for "wired equivalent privacy." Later encryption standards are named "Wi-Fi protected access." As the name implies, the purpose of this form of encryption is to provide protection to the wireless communication channel of similar quality to a wired communication channel.

40. In order to provide a similar level of security to the direct physical connection for the S/Si instruments, the X/Xi instruments must provide additional security controls to protect against attacks that specifically affect wireless communication channels like the RFID at issue here. Without appropriate mitigation measures, wireless communication channels can be susceptible to a number of attacks.

41. One example of such an attack is a passive eavesdropping attack.[5] As with the Wi-Fi example discussed above, it is trivial for an attacker with RFID equipment to read an RFID tag if the communication is not encrypted because, like Wi-Fi, RFID is an open standard. Indeed, attackers can purchase inexpensive RFID tools online.[6] If the

[5] Grassi et. al., *Digital Identity Guidelines*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017 at 45-46, 50, available at: https://doi.org/10.6028/NIST.SP.800-63-3

[6] RFID Readers, AMAZON, available at https://www.amazon.com/RFID-Readers/s?k=RFID+Readers (last visited Jan. 18, 2023); Intuitive-00506505 at -6593.

communication channel is not encrypted, such inexpensive tools can be used to intercept and read the data transmitted between the X/Xi instruments and the robot. The range of most RFID tools can be extended through the use of a more powerful antenna, so the attacker need not be in the same room as the system, making physical security measures – like controlled access areas for use of the robot or spotting an attacker in the room – ineffective.[7]

42. It is also possible to perpetrate active RFID attacks through the use of programmable RFID emitter features of these same tools.[8] Active RFID emitters can have a range of hundreds of meters.[9] These emitters can be programmed to broadcast arbitrary RFID values. In some cases, they can be used in impersonation attacks in which they impersonate another, unsecured, RFID tag.

43. The attacker need not be in the same room or even the same city to perpetrate these types of attacks on an unencrypted RFID channel, as the range of RFID communication can be extended. One such method can be performed by connecting RFID equipment to a small local computer with a connection to a longer-range network such as the Internet. The local computer can then be programmed to send observed RFID tag values to a remote computer over a secure channel such as SSH connection.[10] The remote computer can

[7] GITHUB, *Proxmark3*, available at: https://github.com/Proxmark/proxmark3 (last visited Jan. 18, 2023).
[8] Grassi et. al., *Digital Identity Guidelines*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017 at 39, 48 available at: https://doi.org/10.6028/NIST.SP.800-63-3; Tyler Petersen, *RFID Card Security and Attacks*, (Oct. 15, 2020), SIKITCH, available at: https://www.sikich.com/insight/rfid-card-security-attacks-and-prevention/#:~:text=An%20MITM%20attack%20against%20an,gain%20access%20to%20the%20building.
[9] Annalee Newitz, *The RFID Hacking Underground*, WIRED, (May 1, 2006), available at: https://www.wired.com/2006/05/rfid-2/.
[10] OPENSSH, available at: https://www.openssh.com/ (last visited Jan. 18, 2023).

also control the RFID equipment on the local computer to perpetrate active attacks using the same type of a connection. Such attacks are known as range-extension attacks.

44. A similar and related concept is the concept of impersonating, "spoofing"[11] or "cloning"[12] an RFID tag value. A spoofed RFID tag impersonates another RFID tag by broadcasting the same value as the tag. In many applications, spoofing is not a concern, but in certain types of systems such as RFID-based tracking systems, spoofing is a security issue.

45. Another type of common attack unencrypted wireless channels are susceptible to, is a replay attack.[13] In such an attack, an attacker reads an RFID value and later plays the same value back to a receiver at a different time. In some systems, RFID values change or rotate according to a time schedule. A replay attack allows an attacker to "play back" an earlier tag at a later time. Depending on the design and security of the system, this may allow the attacker to "replay" a value that allows some specific type of access to the system associated with that particular value.

46. I have personally designed and published research on novel anti-spoofing and anti-replay attack-related wireless security systems.[14]

[11] KASPERSKY, *What is Spoofing - Definition and Explanation*, available at: https://www.kaspersky.com/resource-center/definitions/spoofing (last accessed Jan. 18, 2023).
[12] Tyler Petersen, *RFID Card Security and Attacks*, (Oct. 15, 2020), SIKITCH, available at: https://www.sikich.com/insight/rfid-card-security-attacks-and-prevention/#:~:text=An%20MITM%20attack%20against%20an,gain%20access%20to%20the%20building.
[13] Grassi et. al., *Digital Identity Guidelines*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017 at 53, available at: https://doi.org/10.6028/NIST.SP.800-63-3
[14] Martin et. al., *Applications of Secure Location Sensing in Healthcare*, Proceedings of the 7th ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics (2016).

47. The wireless attacks above are not generally applicable to wired systems in the same manner I described above. While it is possible for an attacker to perpetrate such an attack in a wired system, it is more difficult as physical access is required. Therefore, it is important to specifically consider wireless attacks in the design of a wireless system.

48. One way to prevent many types of wireless attacks is through use of cryptographic controls. For example, passive RFID attacks can be prevented by encrypting the tag data. Similarly, encryption or authentication of the tag data can be used to prevent a system from interpreting a false tag data as being from a trusted source.

49. Range extension attacks cannot be prevented entirely through use of cryptography, but their effectiveness can be reduced because an attacker cannot tamper with a cryptographically protected value without knowing the underlying encryption key.

50. Given that Intuitive wirelessly broadcasts essential data—including its counter code and calibration data—using an RFID system in the X/Xi instruments,[15] in my opinion it is both reasonable and necessary to protect that information using cryptography in order to provide a similar level of security to the direct physical connection used to transmit similar information for the S/Si instruments. Further, it is my opinion that it would be illogical to broadcast a counter code that is unprotected, as an unreliable or inauthentic counter code would serve little purpose.

51. The FDA's inquiries to Intuitive emphasize the importance of encryption in preserving wireless data protection and integrity. I understand that the FDA is increasingly focused

[15] Somayaji Dep. Tr. at 56:4–57:23.

on cybersecurity during the review of submissions, and the lack of cybersecurity measures could generate major deficiencies.[16]

52. Consistent with these requirements, the FDA specifically inquired into Intuitive's cybersecurity risk assessment for the X/Xi system, including Xi/Xi instruments. In a submission to the FDA, Intuitive provided its risk assessment that identified a number of identified cybersecurity risks and the mitigation measures Intuitive employed to reduce the likelihood or severity of those risks.[17] One identified risk associated with the RFID reader was that the "[c]ompromise of interface leads to modification of instrument/scope data or injection of false instrument/scope data."[18] The consequences of that type of compromise were listed as (1) "[m]odification of instrument/scope parameters can cause incorrect motion control" and (2) "[p]ossible to use surgical instruments beyond tested life." Both were listed as "Critical" severity, defined as "[c]ompromise of interface can lead to minor or significant surgical or clinical intervention, and results in reversible harm to the patient or user."[19] As a mitigation measure for this identified risk, Intuitive stated, "Communications between RFID reader and tag are encrypted."[20] That reduced the likelihood of the identified risk occurring to "improbable," resulting in a post-risk index of "III: Tolerable Risk."[21] Another identified risk was associated with the RFID tag and described as, "[m]odification of instrument/scope data or injection of false instrument/scope data."[22] The consequences of a compromise of this data were identified

[16] Expert Report of Christy Foreman (Jan. 18, 2023), ¶¶ 246-254.
[17] Intuitive-00499468 at -9640; Intuitive-00506505.
[18] Intuitive-00506505 at -6542.
[19] *Id.* at -6536.
[20] *Id.* at -6542
[21] *Id.*
[22] *Id.*

as follows: (1) "[m]odification of instrument/scope parameters can cause incorrect motion control" and (2) "[p]ossible to use surgical instruments beyond tested life."[23] These consequences also received a "Critical" severity rating.[24] Two mitigation measures were identified that reduced the likelihood to "Improbable" and the post-risk index to "III: Tolerable Risk": (1) "[d]ata on RFID tag are encrypted and password-protected" and (2) "[e]ncryption key and use counting data areas on RFID tag are one-time programmable and cannot be modified once written."[25]

53. This is consistent with my opinions regarding the importance of encryption on wireless communication channels, including the RFID system in the X/Xi instruments, for data of this nature. In testing their RFID security, Intuitive's cyber risk assessment used a RFID reader which, "can be ordered from any popular electronics retail shop."[26] Considering the widespread availably of wireless hacking instruments and the motion control and use counter data stored on Intuitive's RFID chip, the risks of leaving Intuitive's RFID chips unencrypted warranted mitigation steps to reduce the likelihood of those potentially critical risks occurring. Intuitive's RFID testing confirmed that "[n]o observable software faults or security issues were discovered."[27] This included against test cases attempting to "spoof daVinci attachments," "tamper daVinci attachments metadata (use count, identifying data…etc)," and read "sensitive data being passed from the attachment to the daVinci system."[28]

[23] Intuitive-00506505 at -6542.
[24] *Id.*
[25] *Id.*
[26] *Id.* at -6593.
[27] *Id.* at -6594.
[28] *Id.*

VI. THE ATMEL CRYPTORF EEPROM CHIP USED IN THE X AND XI ENDOWRISTS OFFERS SUBSTANTIVE IMPROVEMENTS OVER THE DS2505 EEPROM CHIP

54. In paragraphs 37-59 of his report, Mr. Humphrey purports to explain the reason that Intuitive switched from the wired DS2505 chip in the S/Si EndoWrists to the wireless Atmel chip in the X/Xi EndoWrists.[29] He concludes that the primary purpose of this change was to prevent third parties from adding lives to the X/Xi EndoWrists. As a threshold matter, it would have been entirely possible for Intuitive to add more advanced cryptography to the EndoWrist in a wired design. Switching to a wireless RFID design thus would be unnecessary if the only goal was to provide enhanced cryptographic security to the use counter.

55. In paragraph 38 of his report, Mr. Humphrey reports that, "evidence has not been identified that the Atmel RFID chip offers any substantive improvement over the existing DS2505 chip in operational performance of the X/Xi system."[30] Mr. Humphrey also speculates that the only reason that Intuitive would have made this change is to stop third-party companies from altering the devices.[31]

56. However, evidence of a substantive improvement in the Atmel RFID chip is apparent from a comparison of the data sheets for the two chips. A comparison of the relevant data sheets for the DS2505[32] and the Atmel CrpytoRF[33] chips shows numerous key difference and benefits to the Atmel CryptoRF chip including:

[29] Expert Report of Kurt Humphrey (May 10, 2021), ¶¶ 37-29.
[30] Expert Report of Kurt Humphrey (May 10, 2021), ¶¶ 38.
[31] Expert Report of Kurt Humphrey (May 10, 2021), ¶¶ 47-54.
[32] Dallas Semiconductor DS2505 Data Sheet.
[33] Intuitive-00999731 (Somayaji Deposition, Ex. 224) - Atmel CryptoRF EEPROM Memory Summary Datasheet; Atmel CryptoRF EEPROM Data Sheet.

i. Configuration options for more memory: The Atmel CryptoRF chip is available in more memory configurations and larger memory configurations than the DS2505 chip. This allows for more data to be stored and transferred either as part of the design of the EndoWrist X/Xi or, if not used in this context, allows for easier upgrades in later EndoWrist models that might want to store and transmit more data.

i. Better security features: The Atmel CryptoRF chip supports a range of stronger security features.

ii. High-reliability/high endurance: The CrytpoRF chip advertises a high endurance and high reliability design including 100,000 writes and 10 year data retention. In contrast, the DS2505 data sheet does not list any particular reliability or endurance guarantees.

ii. Integrated tuning capacitor: Unlike the Dallas Chip, the Atmel CryptoRF chip advertises an integrated tuning capacitor.

The Atmel chip also offers up to four times as much storage space and nearly twice as fast data access times than the Dallas chip.[34]

57. Mr. Humphrey also ignores the benefits of wireless technology versus wired technology entirely in his analysis. Wireless technology has numerous benefits over wired.

58. Wired technology requires special care and attention to ensure that wires are routed appropriately in order to minimize repetitive mechanical strain on them (which can cause wires to break over time) and to prevent accidental damage. Similarly, wired technology

[34] Intuitive-00544903 at 5094.

requires special design in connection points, such as where an EndoWrist connects to a da Vinci Robot, in order to ensure that the wire cannot inadvertently become disconnected during use. Wires must also be shielded to prevent RF interference and care must be taken to ensure that they are not defective and that they are connected securely.

59. In contrast, wireless technology has increased reliability against physical damage, as there is no wire that can accidentally break or become disconnected. Wireless technology also tends to have lower manufacturing complexity, as physical concerns related to connecting and routing wiring need not be addressed. This is especially useful in systems such as an EndoWrist where physical mobility has the possibility of damaging or disconnecting the wire or other physical components, reducing reliable operation of the device.[35]

60. Mr. Humphrey dismisses all advantages of wireless chips as "insignificant" in part because Intuitive apparently considered the Dallas Chip as a back-up option. Mr. Humphrey states that, "[o]n the contrary, any possible, yet unstated, performance advantages that might have been anticipated by introducing the RFID chip were insignificant enough that Intuitive used the conventional Dallas chip as their contingency or back-up plan in the event the RFID chip design change failed…the X/Xi EndoWrist module was designed to use either the Dallas chip or the RFID chip without further modifications. Therefore, it appears unlikely that the resulting EndoWrist operational or

[35] Somayaji Dep. Tr. at 81:7-11; Intuitive-00538994 at Tab 19.

mechanical performance would be substantially different, or even distinguishable, regardless of which chip was used."[36]

61. It is my experience that a "fallback" option that exists in case of a supply shortage or other contingencies does not necessarily provide the same performance as the original option. In many cases, the fallback option is compatible, but is lower performing, which is why it is designated as a fallback and not an alternative main option.

62. Furthermore, the conclusion that a fallback option must have insignificant differences to the original option is undermined by the fact that the DS2505 chip does not have RFID and the numerous other functionalities identified above. The "fallback" option therefore is not identical in terms of feature set, and it is unreasonable to assume that the "fallback" option is not "distinguishable" in terms of performance.

63. In my experience, it is extremely common for chips to have the same external interface so that they would fit into the same mechanical design while offering differing performance. Computer central processing unit ("CPUs") are designed this way. For example, Intel supports numerous CPUs with massively differing performance (as determined by core counts, clock speed, overclocking, Turbo Boost, and SMT support) and features that are all pin-compatible with one another, meaning one chip can be directly substituted for another without any changes to the circuit or board layout.[37] Because all processors are pin-compatible it is possible that a slower processor could be used as a "fallback" option for a particular application if a desired model is unavailable. It does not follow that just

[36] Expert Report of Kurt Humphrey (May 10, 2021), ¶¶ 38-39.
[37] *Products Specifications*, INTEL, available at: https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&1_Filter-SocketsSupported=3562 (last visited Jan. 18, 2023).

because the processors are pin-compatible that they have the same performance. Similarly, identifying the Dallas Chip as a "fallback" does not mean that it offered the same benefits as the RFID chip.

64. In paragraph 42 of his report, Mr. Humphrey cites a chart showing a higher instrument failure rate for the da Vinci Xi line of products compared to the da Vinci Si. But as Mr. Humphrey himself admits, "[t]he disclosed RMA/return data details are insufficient to draw any firm conclusions regarding reliability issues associated with replacement of the DS2505 chip in the S/Si EndoWrist instruments with the Atmel CryptoRF chip in the X/Xi EndoWrist instruments."[38] Furthermore, the data that Mr. Humphrey cites do not compare the DS2505 to the Atmel CryptoRF, and they represent a single point in time with no evidence identified by Mr. Humphrey that they would be representative of the entire product life cycle for the X/Xi instruments.

65. Finally, Mr. Humphrey speculates that Intuitive only cared about securing the use counter when making the decision to switch to an RFID interface. He bases this in part on his statement that when Intuitive received information on security concerns with the Atmel chip, "the only concerns [Intuitive] raised were 'about methods to reprogram our RFID's, i.e. change the life-count so that instruments get re-used beyond their design life…'"[39] However, this document appears to post-date the launch of the X/Xi EndoWrists with the RFID technology and the cyber risk assessment referenced above by many years.[40] In his focus on this single email chain reflecting on discussion, Mr. Humphrey ignores other documents, including the cyber risk assessment submitted to the FDA, that also identified

[38] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 42.
[39] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 55.
[40] Intuitive-00861667.

the need for encryption to protect other instrument parameter data that could lead to incorrect motion control of the instruments if compromised.[41]

66. Mr. Humphrey also cites another an email dated years *after* the launch of the X/Xi, where an Intuitive employee notes that "*another possible*" reason to move to X/Xi models is that, "companies have so far only done reprogramming on Si" and "we probably have lead time before they figure out X/Xi."[42] It is not clear how the email would inform or relate to a decision about encryption on a chip for the X and Xi, particularly when that decision substantially predated this email.[43]

VII. BESIDES THE USE COUNTER, THERE ARE OTHER ASPECTS OF THE X/XI ENDOWRISTS THAT USE CRYPTOGRAPHIC CONTROLS

67. There are other aspects of the X/Xi instruments, besides the use counter, that use cryptographic controls. For example, the RFID tag contains calibration information, which is needed for the da Vinci to perform its movements.[44] If this information were tampered with, the da Vinci would not know the correct position of the EndoWrist tip, and its movements would be imprecise.[45] Furthermore, the Tool User ID (TUID) – a number coded for each instrument type – is also encrypted on the RFID chip. This is the number used to generate the drive parameters for the instrument,[46] and changes to this data could pose a safety risk to the patient.[47]

[41] Intuitive-00506505 at -6542.
[42] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 52.
[43] Intuitive-00861667.
[44] Somayaji Dep. Tr. at 63:22–64:12.
[45] Somayaji Dep. Tr. at 110:10-23; Intuitive-00506505 at -542.
[46] Somayaji Dep. Tr. at 59:17–61:15.
[47] Duque 30(b)(6) Dep. Tr. at 40:22–41:1; Intuitive-00506505 at -6542; Somayaji Dep. Tr. at 60:15 - 61:15.

68. Furthermore, the ID was encrypted to both ensure that an unlocked device would not escape an Intuitive manufacturing facility thereby protecting the secrecy of the encryption strategy (a sound precaution if cryptography is to be used at all) and to prevent the data in the RFID from becoming corrupted. [48]

VIII. MR. HUMPHREY'S ANALYSIS OF THE SKYWALKER INSTRUMENTS CONTAINS ERRORS AND ADDRESSES AN IN-PROGRESS DESIGN THAT IS NOT YET FINAL OR CLEARED.

69. Mr. Humphrey contends that "[w]hen recently given the opportunity to select between multiple encryption and connectivity techniques for different types of data, Intuitive chose stronger RF encryption for its use counter while using less robust encryption methods for critical sensor data used to provide haptic feedback to surgeons."[49] Mr. Humphrey then cites the following chart:

4.8 Sensitive Data Flow and Location Table

ID	Sensitive Data Flow Name	Type(s) of Data	PHI/PII Present?	Protected? (Confidentiality)	Protected? (Integrity)	Protected? (Authenticity)	List all Cache / Storage Locations
SD1	Force Feedback Sensor Data	Data collected from physical sensors on the instrument	No	No	Yes (CRC employed)	No	2, 4
SD2	Force Feedback instrument calibration data	Data used for correctly calibrating instrument force feedback functionality	No	Yes	Yes	Yes	2, 3
SD3	Instrument configuration and identification data	Unique instrument id, version, type, and name stored in protected area of secure RFID tag	No	Yes	Yes	Yes	2, 3
SD4	Instrument use count data	Usecount data stored in protected area in secure RFID tag	No	Yes	Yes	Yes	2, 3
SD5	Instrument Authentication Key	Key used for authentication of an instrument to the system	No	Yes	Yes	Yes	3
SD6	Instrument Rootkey	Rootkey for driving instrument specific authentication keys	No	Yes	Yes	Yes	1

[48] Intuitive-00994614.
[49] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 56.

4.4 Reference System Architecture - Communications Path Table

ID	Transport Layer Protocol Name	Application Layer Protocol Name	Protected? (Confidentiality)	Protected? (Integrity)	Protected? (Authenticity)	Sensitive Data	Ref Arch Endpoints	Role
C1	RF	Custom, proprietary	Yes	Yes (employs CRC)	Yes	Yes (instrument configuration, instrument use count, instrument calibration)	2(E1), 3	Communication link between instruments and USM
C2	1-wire	Custom, proprietary	No[1]	No[1]	No[1]	No	2(E2), 4	Supply power to IIFP PIC and transfer information through 1-wire interface

70. He also cites deposition testimony in which the force feedback data used during surgery is described as "exceptionally important" and that it needs to be tamper proof.[50] Mr. Humphrey then states, "Intuitive's 'Cybersecurity System Architecture' provides minimal security to the force feedback data, or the connections that provide that data to the system, and via the system, to the surgeon. For example, the data connection between the force feedback sensors and the system is labeled 'C2' and 'SD1' in the depiction below."[51]

71. There are numerous issues in Mr. Humphrey's analysis. As a threshold matter, assuming that the data referred to is really labeled C2 and SD1, it is important to note that this data is described as being sent over a direct wired pogo-pin connection in the cited deposition testimony. That is, the data is not transmitted wirelessly and is thus not vulnerable to the wireless attacks that I have described above. As such, the design of the transmission of this data uses a different threat model than data that is transmitted wirelessly, and is therefore not necessarily less protected. This is further supported by the table listing the C2 as 1-wire data, and the table earlier in the document (Table 4.3) noting that the, "1-

[50] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 56.
[51] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 57.

wire interface in Gen5 Force Feedback Instrument" has a "Type" of "Wired, Proprietary" and it is the "Interface that connects Gen5 Force Feedback Instrument to DaVinci."[52] The table notes that there is also an "RFID" with a "Type" of "Interface, Wireless, RF" which is the "RFID reader in USM manipulators used for RFID tags in surgical instruments."[53]

4.3 Reference System Architecture - Entry Points / Interfaces Table

ID	Name	Type	Component	Description
E1	RFID	Interface, Wireless, RF	USM	RFID reader in USM manipulators used for RFID tags in surgical instruments
E2	1-wire interface in PSC	Wired, Proprietary	USM	Interface that connects DaVinci to Gen5 Force Feedback Instrument
E3	1-wire interface in Gen5 Force Feedback Instrument	Wired, Proprietary	Gen5 Force Feedback Instrument	Interface that connects Gen5 Force Feedback Instrument to DaVinci

72. Furthermore, it is not clear that Mr. Humphrey has identified the correct data flow. Specifically, the deposition testimony that Mr. Humphrey cites describes force feedback data, but it is not clear if this is describing the sensor data or the calibration data. The calibration data is protected with cryptography.[54] In fact, all data except for the force feedback data is protected with cryptography in this draft design. In my opinion, this is likely because the force feedback data is *wired*. If this data is sent over 1-wire that is one possible reason for this discrepancy, as in that case cryptographic security may not be necessary. That is consistent with the statement in the draft Cybersecurity System Architecture document explaining that protection on the 1-wire communication path "is not required because the connection is a direct local connection."[55] It is also consistent with an internal cybersecurity analysis for Skywalker instruments, which states that

[52] Intuitive-01004385 at -4388.
[53] *Id.*
[54] *Id* at -4389.
[55] Intuitive-01004232 at -4236.

sensor data is transmitted via pogo-pin 1-wire interface, that certain protections are in place to detect changes in data transmitted over this wired connection, and that to circumvent those protections, a sophisticated attacker would need "to insert custom tools in the communication path at the time of the surgery," making the risk improbable.[56]

73. Finally, I understand this relates to an unreleased design for a new EndoWrist product codenamed Skywalker. In my opinion, it is highly improper to review unfinished or incomplete designs and then to draw conclusions about the developers' intentions or the efficacy or level of encryption in the final product. Indeed, I understand that a premarket review submission (called a 510(k)) must be submitted to the FDA for Class II medical devices such as the da Vinci/EndoWrist system and that, as part of the 510(k) review process, the security of the device would be analyzed and thus potentially subject to further iteration or change in order to address FDA's comments and concerns.[57] Mr. Humphrey does not indicate that the design he analyzes is final or that it has undergone the clearance process. It is therefore premature and unreasonable for Mr. Humphrey to review this incomplete design.

IX. REVERSE ENGINEERING X/XI INSTRUMENTS INVOLVES A DIFFERENT PROCESS THAN REVERSE ENGINEERING S/SI INSTRUMENTS.

74. In my opinion, reverse engineering X/Xi instruments involves a different process than reverse engineering the S/Si instruments. Because the X/Xi instruments employ a different security method than the S/Si instruments, the reverse engineering process is also substantially different.[58] This process requires a more sophisticated analysis.

[56] Intuitive-01004242, at -4243.
[57] Expert Report of Christy Foreman (Jan. 18, 2023), ¶¶ 119, 246-254.
[58] Somayaji Dep. Tr. at 109:25-110:6.

Reverse engineering the data stored in a wired chip that lacks encryption does not involve a decryption process, and would instead be more easily accomplished using passive eavesdropping techniques.

75. Though the processes are different, in my opinion, Mr. Humphrey's contentions regarding the extent of the difficulty of reverse engineering the X/Xi instruments are speculative. Mr. Humphrey's analysis appears to be based on a review of documents. Documents may not accurately or fully reflect all implementation details of a device. In my opinion, estimates on reverse engineering difficulty are much more accurate after examining a physical device and attempting to reverse engineer it, and they would vary based on the technical skills and tools used by the engineer. Mr. Humphrey's estimates are not representative of an industry-wide sample, and they do not account for differences in training, experience, or expertise in the reverse engineers engaged in this undertaking.

76. Although I do not attempt to canvas them all here, Mr. Humphrey's July 26, 2021 report, which he calls his "Rebotix Report" and incorporates by reference in Paragraph 19, contains a number of key methodological flaws, one of which undermines his entire analysis.[59] In his Rebotix Report, which forms the basis of how Mr. Humphrey opines that Rebotix would access and reset the Xi use counter, Mr. Humphrey's analysis is predicated on the fact that the data stored on the X/Xi chip is not encrypted at rest.[60]

---

[59] Expert Report of Kurt Humphrey (July 26, 2021) (submitted in the matter of *Rebotix Repair LLC v. Intuitive Surgical, Inc.*, Case No. 8:20-cv-02274 (M.D. Fla.) ("Humphrey Rebotix Report").

[60] For example, Paragraphs 39-41 describe methods to extract a clean image of the data on the CryptoRF chip. Mr. Humphrey then states, "[s]uccessful extraction and analysis of clean images from the CryptoRF EEPROM facilitates straightforward editing/rewriting of the use count and reprogramming an existing X/Xi EndoWrist CryptoRF EEPROM or replacing the existing CryptoRF EEPROM with a new CryptoRF EEPROM personalized with the edited image file." *See* Humphrey Rebotix Report at ¶ 43. Mr. Humphrey also writes, "[t]he user data stored in the Atmel RFID chip can be optionally access and password protected but there is no provision for encrypting stored data internal to the EEPROM block. As

77. However, that premise is not consistent with Intuitive documentation, nor is it consistent with statements made elsewhere in Mr. Humphrey's report. As Mr. Humphrey recognized elsewhere in his report, Intuitive documentation states that the "[d]ata on RFID tag are encrypted and password-protected," and that the "[e]ncyption key and use counting data areas on RFID tag are one-time programmable and cannot be modified once written."[61]

78. Since Intuitive's own documentation and Mr. Humphrey's report contradict the major assumption that Mr. Humphrey's entire reverse engineering analysis depends upon, his analysis is incorrect and his methodology is faulty and unlikely to succeed in practice.

X. CONCLUSION

79. In conclusion, it is my opinion that wireless systems have different security concerns than wired systems, and thus it is necessary to use cryptographic controls on wireless systems to ensure data integrity and security from attackers without a physical presence in the room. Wireless systems have general benefits over wired systems, and specifically the Atmel RFID chip used in the X/Xi EndoWrist X and Xi offers substantive benefits over the DS2505 chip besides the encryption of the use counter. Mr. Humphrey's analysis of the Skywalker instruments is improper because it is an analysis of an in-progress design that has not been finalized or cleared by the FDA. Although reverse engineering the X/Xi instruments involves a different process than reverse engineering the S/Si instruments, Mr. Humphrey's analysis is speculative and contains methodological flaws.

---

previously stated, the only encryption capability available on the CryptoRF chip is during password transmission (through the Authentication Communication setting) and password/user data transmission (through the Encryption Communication mode)." *See* Humphrey Rebotix Report at ¶ 27.

[61] Humphrey Rebotix Report at ¶ 23; Intuitive-00506505 at -6542.

***

All of the facts stated in this report are known personally to me and the opinions proffered are my own. If called as a witness, I could and would testify competently thereto. I declare under penalty of perjury of the laws of the United States that the foregoing is true and correct to the best of my knowledge.

January 18, 2022

Paul D. Martin, Ph.D.

Attachment A

Curriculum Vitae of Paul D. Martin

harborlabs
CYBER.SCIENCE

Paul D. Martin, Ph.D.

443.449.9006
paul@harborlabs.com
1777 Reisterstown Road, East Bldg, Suite 230; Pikesville, MD 21208

Profile

Dr. Martin is the Director of Firmware Security and a Senior Research Scientist at Harbor Labs. His research interests include embedded system security, operating system security, vulnerability analysis, reverse engineering, network protocol analysis, applied cryptography, cryptanalysis and privacy-preserving protocols.

Education

2011-2016	*Ph.D. Computer Science Johns Hopkins University Baltimore MD* *Securing Medical Devices and Protecting Patient Privacy in the Technological Age of Healthcare*	
2011-2013	*M.S.E. Computer Science Johns Hopkins University Baltimore MD*	
2007-2011	*B.S. Computer Science Johns Hopkins University Baltimore MD*	

Industry Experience

2018-Present	*Harbor Labs*	**Director of Firmware Security, Senior Research Scientist**
2013-2018	*Harbor Labs*	**Research Scientist**
2011-2016	*Johns Hopkins University Health and Medical Security Lab*	**PhD Candidate, Research Assistant**
2013	*Applied Communication Sciences*	**Graduate Intern**
2011	(ICPSR) *University of Michigan Inter-university Consortium for Political and Social Research*	**Penetration Tester**
2009-2011	*Independent Security Evaluators*	**Security Intern**
2008-2010	(DRCC) *Johns Hopkins University Digital Research and Curation Center*	**Student Programmer**
2008	*Brandeis University Hardware Repair Shop*	**Freelance Programmer**

Teaching Experience

2015	*Introduction to Hardware Hacking*	**Instructor**
2012-2014	*Security and Privacy*	**Teaching Assistant**
2011	*Practical Cryptographic Systems*	**Course Assistant**

Publications

P. Mart n, D. Russe , M. Ben Sa em, S. Checkoway, A. Rub n, Sent ne : Secure Mode Prof ng and Enforcement for Embedded Systems, Proc. ACM/IEEE Internat ona Conference on Internet-of-Th ngs Des gn and Imp ementat on, (IoTDI 18).

P. Mart n, M. Rushanan, T. Tant o, C. Lehmann and A. Rub n, App cat ons of Secure Locat on Sens ng n Hea thcare. In the proceed ngs of ACM Conference of B o nformat cs, Computat ona B o ogy, and Hea th Informat cs (BCB 16).

harborlabs
CYBER.SCIENCE

J. Carr gan, P. Mart n, M. Rushanan, KBID: Kerberos Brace et Ident f cat on. In the Proceed ngs of F nanc a Cryptography and Data Secur ty (FC 16).

P. Mart n, M. Rushanan, S. Checkoway, M. Green, A. Rub n. C ass fy ng Network Protoco Imp ementat on Vers ons: An OpenSSL Case Study. Techn ca Report 13-01, Johns Hopk ns Un vers ty (December 2013).

P. Mart n, A. Rub n, and R. Bhatt , *Enforcing Minimum Necessary Access in Healthcare Through Integrated Audit and Access Control.* In ACM Conference on B o nformat cs, Computat ona B o ogy, and B omed ca Informat cs Hea th Informat cs Sympos um (BCB-HIS), (September 2013)

Patents

System and Method for automat ca y extract ng nformat on from b nary f es for use n Database Quer es	**US 10,762,214 B1**
System and method for network traff c prof ng and v sua zat on	**US 9,667,521 B2**
System and method for network traff c prof ng and v sua zat on (Pend ng)	**US 15/606,717**
System and method for network traff c prof ng and v sua zat on (Pend ng)	**WO 2015113036A1**
Hea thcare pr vacy breach prevent on through ntegrated aud t and access contro	**US 8,984,583 B2**
Hea thcare pr vacy breach prevent on through ntegrated aud t and access contro	**US 9,438,632 B2**

Current Research

Automated b nary vers on extract on for NVD cross-reference based on fuzzy match ng.
Automated ana ys s of vu nerab t es n conta ners and v rtua app ances.
Large-sca e compar son of nature and k nd of f rmware vu nerab t es across and w th n product c asses.

Expert Witness Engagements

Un ted States **v. Laffon Ellis**

Case:	Case # 2:19-cr-00369-DWA
Descr pt on:	Ana ys s re ated to re ab ty of spec f c types of computer zed DNA ana ys s n cr m na proceed ngs.
Serv ces:	Source code rev ew. Expert report draft ng.
Expert Test mony at Hear ng:	Monrov a, MD (December 20, 2021)

Sysmex Corporat on and Sysmex Amer ca, Inc. v. **Beckman Coulter, Inc.**

Case:	CA # 19-1642-RGA-CJB
Descr pt on:	L t gat on re ated to hemato ogy ana ys s mach ne patents.
Serv ces:	Source code rev ew. Expert report draft ng.
Expert Test mony at Depos t on:	Monrov a, MD (November 22, 2021)

CERTAIN ROUTERS, ACCESS POINTS, CONTOLLERS, NETWORKS MANAGEMENT DEVICES, OTHER NETWORKING PRODUCTS, AND HARWARE AND SOFTWARE COMPONENTS THEREOF

Case:	ITC Invest gat on No. 337-TA-1227
Descr pt on:	ITC Invest gat on re ated to patents on w re ess network handoff, network management and QoS techno og es.
Serv ces:	Source code rev ew. Va d ty and pr or art ana ys s. Expert report draft ng.
Expert Test mony at Tr a :	Wash ngton, DC (Ju y 28, 2021)
Expert Test mony at Depos t on:	Monrov a, MD (June 9-10, 2021)

Micro Focus, Inc. v. Insurance Serv ces Organ zat on

Case:	DE C v Act on # 15-252-RGA
Descr pt on:	L t gat on re ated to un censed use of runt me env ronments,

harborlabs
CYBER.SCIENCE

brar es and software comp ers.
Serv ces: Source code rev ew. B nary reverse eng neer ng and ana ys s. Aff dav t draft ng. Expert report draft ng.
Expert Test mony at Depos t on: Monrov a, MD (Feb 2, 2021)

loanDepot.com, LLC v. S gma Infoso ut ons, Inc.
Case: AAA Case # 01-18-0001-5821
Descr pt on: L t gat on re ated to software deve opment pract ces.
Serv ces: Source code ana ys s, exper mentat on, report draft ng.
Expert Test mony at Depos t on: Ba t more, MD (December 17, 2019)

Cypress Lake Software, Inc. v. Samsung E ectron cs Amer ca and De , Inc.
Case: Case # 6:18-cv-00030-RWS
Descr pt on: L t gat on re ated to nfr ngement of UX patents.
Serv ces: Source code ana ys s, report draft ng.
Expert Test mony at Depos t on: Ba t more, MD (Ju y 9, 2019)

Apple, Inc. Device Performance Litigation
Case: CA C v Act on # 18-md-02827-EJD
Descr pt on: L t gat on re ated to bus ness pract ces.
Serv ces: Techn ca ana ys s and expert reports on secur ty and techn ca aspects of mob e phone forens cs.

Ita an Ant trust Author ty v. **Apple, Inc.**
Case: PS/11309
Descr pt on: L t gat on re ated to bus ness pract ces.
Serv ces: Techn ca ana ys s and expert reports on secur ty and techn ca aspects of software update processes.

Carl Zeiss AG and ASML Netherlands B.V. v. N kon
Case: Case # 2:17-cv-07083-RGK (MRWx)
Descr pt on: L t gat on re ated to patents on mage detect on a gor thms.
Serv ces: Code rev ew of a gor thms re ated to mage process ng and detect on a gor thms. Dec arat on on aspects of source code rev ew process.

Dec s on Resources, LLC v. **Brigham Hyde, Precision Health Intelligence, LLC and Orr Inbar**
Case: MA C v Act on # 17-2834J
Descr pt on: L t gat on re ated to t me ne of software deve opment and m sappropr at on of trade secrets.
Serv ces: Source code and documentat on rev ew, t me ne deve opment. Aff dav t draft ng.

Litigation Support

WSOU Investments, LLC. v. M crosoft Corporat on
Case: Case # 1:18- 6:20-cv-00464-ADA, 6:20-cv-00460-ADA, 6:20-cv-00457-ADA,
Descr pt on: L t gat on re ated to patents on te ephony management systems and sk -based matchmak ng.
Serv ces: Source code rev ew and documentat on rev ew, va d ty ana ys s, nfr ngement ana ys s, report draft ng.

10Tales Inc. v. T kTok PTE. Ltd.
Case: Case # 1:18-cv-826-WCB
Descr pt on: L t gat on re ated to patents on user-adapted v deo streams.
Serv ces: C a m construct on ana ys s.

harborlabs
CYBER. SCIENCE

Carr ere v. **Symantec Corporation**

Case:	Case # 500-06-000894-176
Descr pt on:	C ass act on t gat on re ated to product secur ty.
Serv ces:	Source code rev ew, documentat on rev ew, report draft ng.

IOENGINE, LLC v. Ingen co, Inc.

Case:	Case # 1:18-cv-826-WCB
Descr pt on:	L t gat on re ated to patents on payment process ng systems.
Serv ces:	Source code rev ew and documentat on rev ew, va d ty ana ys s, nfr ngement ana ys s, report draft ng.

IOENGINE, LLC v. PayPa Ho d ngs, Inc.

Case:	Case # 1:18-cv-452-WCB
Descr pt on:	L t gat on re ated to patents on payment process ng systems.
Serv ces:	Source code rev ew and documentat on rev ew, va d ty ana ys s, nfr ngement ana ys s, report draft ng.

AGIS Software Deve opment LLC v. **Uber Technologies**

Case:	Case # 2:21-cv-00026-JRG-RSP
Descr pt on:	L t gat on re ated to patents on map over ays and messag ng systems.
Serv ces:	Source code rev ew.

F njan v. **Palo Alto Networks**

Case:	Case # 4:14-CV-04908-PJH
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways.
Serv ces:	Inva d ty ana ys s, C a m construct on ana ys s, source code rev ew.

Huawe Techno og es Co. v. **Verizon Communications Inc.**

Case:	Case # 6:20-CV-00090
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways w th c oud components.
Serv ces:	Source code rev ew, non- nfr ngement ana ys s.

Ep c Games, Inc. vs. **Apple, Inc.**

Case:	Case # 4:20-cv-05640-YGR-TSH
Descr pt on:	L t gat on re ated to bus ness pract ces.
Serv ces:	Document rev ew, nterv ews, report draft ng.

Ph ps North Amer ca LLC ; Kon nk ujke Ph ps N.V. vs. **Summit Imaging Inc.**

Case:	Case # 2:19-cv-01745-JLR
Descr pt on:	L t gat on re ated to th rd-party repa r serv ces.
Serv ces:	Source code rev ew, document rev ew, report draft ng.

California Physicians Service, Inc D/B/A Blue Shield of California vs. Hea thp an Serv ces Inc,

Case:	Case # 3:18-cv-3730
Descr pt on:	L t gat on re ated to software deve opment pract ces and breech of contract.
Serv ces:	Document rev ew, source code rev ew, report draft ng.

F njan v. **Qualys**

Case:	Case # 4:18-cv-07229-YGR
Descr pt on:	L t gat on re ated to patents on vu nerab ty assessment products.
Serv ces:	Inva d ty ana ys s, Non- nfr ngement ana ys s, source code rev ew, report draft ng.

F njan v. **Sonicwall**

harborlabs
CYBER. SCIENCE

Case:	Case # 5:17-cv-04467-BLF-HRL
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways.
Serv ces:	Inva d ty ana ys s, Non- nfr ngement ana ys s, source code rev ew, report draft ng.

TecSec Inc. v. C sco and Orac e

Case:	Case # 1:10-cv-115 LO-TCB
Descr pt on:	L t gat on re ated to patents on hardware acce erated cryptograph c processors.
Serv ces:	Infr ngement ana ys s, va d ty ana ys s, source code rev ew, report draft ng.

Blackberry Limited v. Facebook, Inc.

Case:	Case # 2:18-cv-01844-KSx
Descr pt on:	L t gat on re ated to patents on agent-based network mon tor ng, conf gurat on and secur ty systems.
Serv ces:	Infr ngement ana ys s, va d ty ana ys s, source code rev ew, report draft ng.

Un oc, Inc. v. **Big Fish Games, Inc.**

Case:	Case # 2:16-cv-00741-JRG
Descr pt on:	L t gat on re ated to patents on hardware cryptograph c ch ps.
Serv ces:	Non- nfr ngement ana ys s, report draft ng, source code rev ew.

SPEX Techno og es, Inc. v. **Toshiba America Electronic Components, Inc., et al.**

Case:	Case # 8:16-cv-01800-JVS
Descr pt on:	L t gat on re ated to patents on hardware cryptograph c ch ps.
Serv ces:	Non- nfr ngement ana ys s, report draft ng.

Symantec Corporation v. Zsca er, Inc.

Case:	Case # 3:17-cv-04414-JST,
Descr pt on:	L t gat on re ated to patents on secur ty gateways, URL f ter ng and categor zat on
Serv ces:	Infr ngement ana ys s, ass gnor estoppe , document rev ew.

Kon nk jke Ph ps v. **Microsoft Inc.**

Case:	Case # 4:18-cv-01885-HSG,
Descr pt on:	L t gat on re ated to patents on secure cryptograph c protoco s
Serv ces:	Non- nfr ngement ana ys s, va d ty ana ys s, c a m construct on ana ys s, document rev ew, source code rev ew.

Netfuel, Inc. v. C sco Systems, Inc.

Case:	Case # 5:18-cv-2352-EJD
Descr pt on:	L t gat on re ated to patents on agent-based network mon tor ng, conf gurat on and secur ty systems.
Serv ces:	Infr ngement ana ys s, c a m construct on ana ys s, source code rev ew, report draft ng.

Byrd et al. v. Aaron s, Inc., et a .

Case:	PA C v Act on # 1:11-cv-00101-SJM-SPB
Descr pt on:	C ass act on t gat on re ated to pr vacy.
Serv ces:	Attend depos t ons, source code rev ew, report draft ng.

F njan v. **Juniper Networks**

Case:	Case # 3:17-cv-05659-WHA
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways.
Serv ces:	Inva d ty ana ys s, non- nfr ngement ana ys s, source code rev ew.

harborlabs
CYBER. SCIENCE

Grace et a . v. **Apple Inc.**

Case:	Case # 5:17-cv-00551-LHK (NC)
Descr pt on:	L t gat on re ated to dev ce performance and serv ce outages.
Serv ces:	Mob e forens cs and dev ce ana ys s, report draft ng, source code rev ew, document rev ew, techn ca ana ys s and argument construct on.

Rimini Street, Inc. v. Orac e Internat ona Corporat on, et a .

Case:	Case # 2:14-cv-01699 LRH-CWH
Descr pt on:	L t gat on re ated to fa se c a ms on secur ty.
Serv ces:	Large-sca e test ng of IPS techn ques for nc ud ng custom test nfrastructure and mp ementat on of techn ques to b ock exp o tat on of vu nerab t es, techn ca ana ys s of vu nerab t es.

F njan v. **Symantec Corporation**

Case:	Case # 14-cv-02998-HSG
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways, endpo nt protect on and f rewa s.
Serv ces:	Bu d and/or test software for W ndows, nva d ty argument strategy, non- nfr ngement argument strategy, report preparat on, source code rev ews.

Str keforce, Inc. v. **Entrust et al.**

Case:	Case # 1:17-cv-00309
Descr pt on:	L t gat on re ated to patents on authent cat on techno og es.
Serv ces:	Inva d ty argument deve opment, non- nfr ngement argument deve opment, report draft ng.

Sony Corporation, Inc. v. Arr s

Case:	Inv. # 337-TA-1049
Descr pt on:	L t gat on re ated to patents on te ev s on stream ng dev ces and/or serv ces.
Serv ces:	Va d ty argument deve opment, source code rev ew of ent re p atform codebase nc ud ng numerous embedded p atforms, nfr ngement argument deve opment.

Kudelski SA, Nagra USA, Inc., Nagravision SA, and OpenTV, Inc. v. Comcast Corporat on

Case:	Case # 2:16-cv-1362-JRG, Inv. # 337-TA-1049
Descr pt on:	L t gat on re ated to patents on te ev s on stream ng dev ces and/or serv ces.
Serv ces:	Va d ty argument deve opment, source code rev ew of ent re p atform codebase nc ud ng numerous embedded p atforms, nfr ngement argument deve opment.

Amazon.com Inc., Hulu, LLC, and Netflix, Inc. v. Un oc Luxembourg S.A.

Case:	IPR 2017-00948
Descr pt on:	L t gat on re ated to patents on DRM protect on for content d str but on
Serv ces:	Pr or art search, PGR Preparat on, IPR preparat on.

Ph shMe v. **Wombat Technologies, Inc.**

Case:	Case # 16-403-LPS-CJB
Descr pt on:	L t gat on re ated to patents on ant -ph sh ng tra n ng techno og es.
Serv ces:	Pr or art search, PGR Preparat on, IPR preparat on.

Nader Asghar -Kamran and Kamran Asghar -Kamran v. **United States Automobile Association**

harborlabs
CYBER.SCIENCE

Case: Case # 2:15-cv-478
Descr pt on: L t gat on re ated to patents on authent cat on techno og es.
Serv ces: Pr or art search, nva d ty argument strategy, non- nfr ngement argument strategy, source code rev ews

V r2us v. **Invincea Inc. and Invincea Labs, LLC**
Case: Case # Case 2:15-cv-00162-HCM-LRL
Descr pt on: L t gat on re ated to patents on v rtua zat on and automated corrupt on repa r.
Serv ces: Pr or art search, nva d ty argument strategy, non- nfr ngement argument strategy, source code rev ews

Palo Alto Networks v. F njan
Case: IPR 2016-00159, IPR 2016-00151, IPR 2015-01974, IPR 2015-02001, IPR 2015-01979
Descr pt on: L t gat on re ated to patents on ma ware scann ng gateways and f rewa s,
Serv ces: Pr or art search, patent nterpretat on, IPR preparat on support, c a m chart rev ew

TVIIM v. **McAfee**
Case: Case # 3:13-cv-04545-VC
Descr pt on: L t gat on re ated to patents on vu nerab ty scann ng
Serv ces: Bu d and test software for SPARC/L nux/W ndows, patch out cense checks/crack software (w th perm ss on), obta n hard-to-f nd egacy software, pr or art and non-nfr ngement argument strategy support, source code rev ews, pr or art search

Al Cioffi et al. v. Goog e
Case: Case # 2:13-cv-103-JRG-RSP
Descr pt on: L t gat on re ated to patents on browser sandbox ng and process so at on.
Serv ces: Code rev ew/software test ng to co ect ev dence of nfr ngement, Infr ngement argument preparat on support, c a m chart rev ew

Rovi Solutions & Veracode v. Appthor ty
Case: Case # 12-10487-DPW
Descr pt on: L t gat on re ated to patents on stat c debugg ng too s
Serv ces: Source code rev ew refut ng oppos ng expert test mony

Pre-Harbor Labs Security Design and Software Development Experience

2013 At *Applied Communication Sciences*
Ro e: Graduate Intern
Techno og es: JavaScr pt, Python, Tcpdump, W reshark

- Deve oped extens b e rea -t me traff c v sua zat on too to chart and ana yze h gh-vo ume tcpdump streams of ossy metropo tan-area mesh network traff c.

2011 At *University of Michigan ICPSR*
Ro e: Penetrat on Tester
Techno og es: Numerous Secur ty Too s, Amazon EC2, VMware VSphere

- Conducted w de-sca e penetrat on test ng on v rtua zed c oud-based systems meant to be secure

harborlabs
CYBER.SCIENCE

env ronments for researchers to store conf dent a resu ts
- Created forma threat mode document deta ng potent a secur ty vu nerab t es from a poss b e attack vectors
- Wrote two reports deta ng resu ts from penetrat on test

2009-2011 At *Independent Security Evaluators*
Ro e: Secur ty Intern
Techno og es: C++, C#, Da v k Bytecode, Gcov, GDB, Javascr pt, Peach Fuzzer, Python, RegEx, XML, W reshark

- Created og pars ng framework to ana yze 20+ og f e formats
- Ass sted w th ma ware test ng, research and ana ys s
- Reverse eng neered DRM schemes n Andro d and IOS app cat ons
- Researched and prototyped secure cryptograph c ma de very system
- Deve oped web craw er to co ect f e sets for use n fuzz ng
- Wrote code-coverage ana ys s too for construct ng m n mum f e set for fuzz test ng
- Wrote fuzz ng p ug ns us ng Peach Fuzzer framework and reverse eng neered b nary f e spec f cat ons
- Wrote Internet Exp orer and Chrome extens ons for cryptograph c proxy system
- Created and debugged network protoco s for use n network protoco test ng
- Wrote and debugged un t tests n C++ and Python for propr etary d sk-encrypt on system

2008-2010 At *Johns Hopkins University DRCC*
Ro e: Student Programmer
Techno og es: DOM, Java EE, JSP Per , SAX, XSLT

- Drafted a report deta ng secur ty recommendat ons for an NSF funded data conservancy project
- Set up and dep oyed a Fedora d g ta repos tory w th the Is andora frontend
- Ported IRStats stat st cs package to the DSpace nformat on repos tory XMLUI
- Wrote batch mporter that s now used to mport more than 20 d g t zed books a week nto DSPace repos tory

2008 At *Brandeis University Information Technology Services Hardware Repair Shop*
Ro e: Free ance Programm ng Consu tant
Techno og es: Java, V sua C++, VBScr pt

- So e programmer on project to nterface Request Tracker t cket ng system w th Brother PT- 9500PC Labe Pr nter

Technical Skills

Languages	BASH, C, C++, C#, HTML, Java, JavaScr pt, Object ve-C, MATLAB, Python, Per , PHP, Regu ar Express ons, SQL, XML
Architectures	6502, 8051, 8080, ARM Cortex-M, ARMv7, ARMv8, AVR, m68k, MIPS, MSP430, PIC, SPARC, PowerPC, x86, x86-64, Z80
Operating Systems	Andro d, ChromeOS, FreeBSD, OS, OpenBSD, L nux, macOS, W ndows
DevOps and Development Tools	Ans b e, Ant, B tBucket, Conf uence, Docker, gdb, g t, G tHub, G tLab, Grad e, Hadoop, jad, jd-gu , J ra, Maven, make, MySQL, PostgreSQL, subvers on, Tre o, Vagrant, va gr nd
Security Tools	A rcrack-ng, apktoo , b nwa k, bu k-extractor, Burp su te, Char es Proxy, cur , dex2jar, ftk, hashcat, IDA Pro,

harborlabs
CYBER.SCIENCE

Cloud and Virtualization	Metasp o t, m tmproxy, Nessus, nmap, OpenSSL, ophcrack, p0f, Sca pe , sk pf sh, snort, ss str p, ss yze, Vo at ty, Web Scarab, wget, W reshark AWS, Azure, Bhyve, KVM, LXD, QEMU, v rt-manager, VMware, Xhyve

Honors, Societies and Awards

- Member Ups on P Eps on Internat ona Computer Sc ence Honor Soc ety
- Member Inst tute for E ectr ca and E ectron cs Eng neers (#97507890)
- Member Assoc at on for Comput ng Mach nery (#9700346)

At Johns Hopkins University

- Computer Sc ence Department Outstand ng Teach ng Ass stant Award
- Treasurer, Ups on P Eps on Internat ona Computer Sc ence Honor Soc ety (JHU Chapter)
- Computer Sc ence Department Facu ty L a son Czar
- Student Representat ve to the Computer Sc ence Undergraduate P ann ng Curr cu um Comm ttee

Attachment B

Materials Considered

Case Documents

Pleadings

- Complaint, *Surgical Instrument Service Co., Inc. v. Intuitive Surgical, Inc.*, No. 3:21-cv-03496-VC (ECF 1) (May 10, 2021)
- Consolidated Amended Class Action Complaint, *In re: da Vinci Surgical Robot Antitrust Litigation*, Lead Case No. 3:21-cv-03825-VC (ECF 52) (Sept. 9, 2021)

Expert Reports

- Expert Report of Christy Foreman (Jan. 18, 2023)
- Expert Report of Kurt Humphrey (May 10, 2021)
- Expert Report of Kurt Humphrey, submitted in the matter of *Rebotix Repair LLC v. Intuitive Surgical, Inc.*, Case No. 8:20-cv-02274 (M.D. Fla.) and dated July 26, 2021

Deposition Transcripts and Exhibits

- Deposition of Grant Duque 30(b)(6) (November 8, 2022)
- Deposition of Grant Duque (November 8, 2022)
- Deposition of Sharathchandra "Shark" Somayaji (November 4, 2022)
- Deposition of Margaret Nixon (October 7, 2022)

Produced Documents

- Intuitive-00002201 - da Vinci Si Surgical System User Manual
- Intuitive-00002502 - da Vinci Xi System User Manual
- Intuitive-00499468
- Intuitive-00506505
- Intuitive-00538994
- Intuitive-00544903
- Intuitive-00861667
- Intuitive-00994614
- Intuitive-00999731 (Somayaji Deposition, Ex. 224) - Atmel CryptoRF EEPROM Memory Summary Datasheet
- Intuitive-01004232
- Intuitive-01004242
- Intuitive-01004385

Other Documents

- Annalee Newitz, *The RFID Hacking Underground*, WIRED, (May 1, 2006), available at: https://www.wired.com/2006/05/rfid-2/.
- Atmel CryptoRF EEPROM Data Sheet.
- Dale Anderson, *Understanding Crypto Memory the World's Only Secure Serial EEPROM*, ATMEL (2004).
- Dallas Semiconductor DS2505 Data Sheet.
- GITHUB, *Proxmark3*, available at: https://github.com/Proxmark/proxmark3 (last visited Jan. 18, 2023).
- Grassi et. al., *Digital Identity Guidelines*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017, available at: https://doi.org/10.6028/NIST.SP.800-63-3.
- KASPERSKY, *What is Spoofing - Definition and Explanation*, available at: https://www.kaspersky.com/resource-center/definitions/spoofing (last accessed Jan. 18, 2023).
- Martin et. al., *Applications of Secure Location Sensing in Healthcare*, Proceedings of the 7th ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics (2016).
- OPENSSH, available at: https://www.openssh.com/ (last visited Jan. 18, 2023).
- Products Specifications, INTEL, available at: https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&1_Filter-SocketsSupported=3562 (last visited Jan. 18, 2023).
- RFID Readers, AMAZON, available at https://www.amazon.com/RFID-Readers/s?k=RFID+Readers (last visited Jan. 18, 2023).
- Tyler Petersen, *RFID Card Security and Attacks*, (Oct. 15, 2020), SIKITCH, available at: https://www.sikich.com/insight/rfid-card-security-attacks-and-prevention/#:~:text=An%20MITM%20attack%20against%20an,gain%20access%20to%20the%20building.

Exhibit 3

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SURGICAL INSTRUMENT SERVICE COMPANY, INC. Plaintiff/Counter-Defendant	) Civil Action No.:) 3:21-cv-03496-VC
Vs.	)
INTUITIVE SURGICAL, INC., Defendant/Counterclaimant	)

HIGHLY CONFIDENTIAL ATTORNEYS' EYES ONLY

Deposition of PAUL D. MARTIN, Ph.D., was taken via videotape and Zoom on Thursday, March 16, 2023, commencing at 10:32 a.m., at 12102 Ashcroft Terrace, Monrovia, Maryland, before MICHELE D. LAMBIE, Notary Public.

Reported By:

Michele D. Lambie, CSR-RPR

APPEARANCES:

ON BEHALF OF THE PLAINTIFF/COUNTER-DEFENDANT:

McCaulley Law Group.

JOSHUA VAN HOVEN, ESQUIRE.

josh@mccaulleylawgroup.com.

3001 Bishop Drive.

Suite 300.

San Ramon, California 94583.

(925) 302-5941

ON BEHALF OF THE DEFENDANT/COUNTERCLAIMANT:

Covington & Burling LLP.

KATHRYN ELIZABETH CAHOY, ESQUIRE.

kcahoy@cov.com.

3000 El Camino Real.

5 Palo Alto Square.

Palo Alto, California 94306.

(650) 632-4700

APPEARANCES CONTINUED:

ON BEHALF OF THE DEFENDANT/COUNTERCLAIMANT:

Covington & Burling LLP.

MIRIAM ARGHAVANI, ESQUIRE.

marghavani@cov.com.

415 Mission Street.

Suite 5400.

San Francisco, California 94105.

(415) 591-7059

ALSO PRESENT: Nolan Church - Videographer

Paul Baker - Concierge

EXAMINATION INDEX

EXHIBITS INDEX

(Attached to Transcript.)

the datasheet up. That's why I'm not super comfortable without doing that. It's always best to do that.

Q. We're -- we're waiting for the internet. Just -- I don't think we need a -- a break though. Just give me a second here as I get this specific document up.

(Brief pause.)

BY MR. VAN HOVEN:

Q. Okay. Who is Atmel?

A. What? I'm sorry, I didn't hear you.

Q. Sorry, yeah. Who is Atmel?

A. They're a company.

Q. What type of company are they?

A. They make chips, generally speaking. At least I know of the chips they make, microcontrollers and other types of chips as well.

Q. And the Dallas DS2505 chip, do you know who makes that chip?

A. So, I'd like to see the data chip for that -- datasheet for that chip, too.

I really prefer to see the datasheets whenever we're talking about chips. There's a lot of room for blending things together otherwise.

Q. Are there a number of suppliers of RFID chips?

A. Yes.

Q. About how many do you think?

A. I could not put an estimate on it.

Q. More than five?

A. Yeah, probably.

Q. Quite a few?

A. Yeah. I mean, I don't know what you mean by quite a few, but there's -- there are -- there are -- I could think of several.

Q. Are there a number of suppliers of wired EEPROM chips?

A. Yes.

Q. More than five?

A. Yes.

Q. Again, quite a few?

MS. CAHOY: Objection to form.

THE WITNESS: The same answer. I'm not sure what you mean by quite a few, but I would say that I'm familiar with many. Like, you know, more than -- more than five certainly suppliers of EEPROM chips I have seen in different examples in my life.

BY MR. VAN HOVEN:

Q. Are RFID chips commodity components?

MS. CAHOY: Objection to form.

THE WITNESS: It depends on your definition of commodity.

BY MR. VAN HOVEN:

Q. There are a lot of suppliers of relatively interchangeable parts with a lot of different specifications?

MS. CAHOY: Objection to form.

THE WITNESS: For certain types of RFID chips, that is true.

BY MR. VAN HOVEN:

Q. What about wired EEPROM chips, are those commodity parts?

A. It's the same answer. So, generally speaking if you're just referring to a generic EEPROM with no other special properties, sure, but, you know, there might be specialized EEPROMS that are -- that have special features, and then they wouldn't be commodity parts. So, it really depends.

You'd have to provide a specific example, but I could say there are many EEPROMS, and many of them are compatible with one another.

Q. I think that I may have beat the internet and get this thing up.

A. Yeah.

(Whereupon, Martin Deposition Exhibit No. 23, Atmel Summary Datasheet, Marked for identification.)

BY MR. VAN HOVEN:

Q. If you could take a look at we've marked as Exhibit 23.

A. I recognize this one, and I am -- yeah, I recognize this one.

Q. Okay. Is -- based on this, do you have an understanding as to whether the Atmel RFID chip used in Xi EndoWrists is an active or passive tag?

A. Yes.

Q. What's your understanding?

A. Wait. This datasheet only has 11 pages.

Q. That's the -- that's the number that you provided me in your report for RFID.

A. Okay. This might be not --

Q. You can go back to the other one that we had, too, if you want.

A. I'll just -- I'll just use the other one. While you were talking, I flipped through it, and it seems to have a lot of the things that I want to refer to for this discussion.

Q. Okay. So, I'll get Exhibit 22 back up, if I can figure out how to do that.

A. Okay. Okay.

Q. Do you have an understanding of whether the Atmel RFID tag used in the Xi EndoWrist is an active or passive tag?

A. I do.

Q. What's your understanding?

A. Sure. Just give me a second to point to where I want to here.

So, if you look under Description in paragraph 2, it describes that the RF interface powers the other circuits; no battery is required.

So, based on how we're using the term in this case, which is a fairly common usage, it's a passive tag. Though, I do note that it's referred to as having an active state, and that's where some confusion can come in, but I would define this as a passive tag.

Q. And -- and so is it your understanding that in the context of a -- of a -- well, okay. Strike that.

An Xi robot, as you understand it, has a reader that is able to interface with the RFID tag in an Xi EndoWrist; is that right?

A. That's my understanding.

Q. And the reader is a device that lights up

the RFID tag via a wireless signal, is that how you understand that to work?

A. That's part of what it does.

Q. Assuming that the RFID reader within the robot arm is -- is providing that signal to light up the tag and the tag is in proximity of the arm, will the -- will the tag light up and respond?

A. It should.

Q. It wouldn't need to be attached to do that, would it?

A. The tag is attached to the arm.

Q. I mean, the arm -- the -- the EndoWrist wouldn't need to be attached to the arm for the tag to respond, assuming the reader is sending a signal?

MS. CAHOY: Objection to form.

THE WITNESS: Oh, I see. The answer is it probably wouldn't, but I could think of a few configurations in which you could design -- design a device where that wouldn't be true necessarily, but it shouldn't.

BY MR. VAN HOVEN:

Q. But -- yeah, absent one of those special kind of configurations, as long as you're within the range of whether it's three inches or six inches, it should light up and activate and respond?

A. With the caveat, I haven't tested this, but it should.

Q. Can we go to -- actually, let's go into something else. What's a -- have you ever heard the term whitelist in the context of information security?

A. Yes.

THE WITNESS: But just to pause. If we're going into something else, depending on how something else, how long it is, it might be a good time for lunch.

MR. VAN HOVEN: Yeah, no. Yeah, you're -- you're getting late into your -- so, yeah. Why don't we take a little break or a longer break.

Mr. Shafer?

A. No.

Q. I'd like to talk a little bit about the use counter on the Xi EndoWrist, okay?

A. Did you say Xi?

Q. Yes, Xi, the -- the more recent generation.

A. Okay. Sure.

Q. And do you understand that the use counter value is stored on the Atmel CryptoRF chip that we've been discussing within an Xi EndoWrist?

A. Yes.

Q. Do you know if that use counter value is stored at a kind of particular region of memory within the Atmel CryptoRF chip?

A. It is stored within a particular region of memory.

Q. Do you have an understanding as to whether that region of memory is read only?

A. Give me one second, please.

(Whereupon, there was a pause for

document examination.)

THE WITNESS: I'm still examining parts of the report, so please just give me a little bit more time.

BY MR. VAN HOVEN:

Q. No problem.

(Whereupon, there was a pause for document examination.)

THE WITNESS: Okay. Apologies still. Because there's no search, it's taking me just a little bit longer.

(Whereupon, there was a pause for document examination.)

THE WITNESS: Okay. Now, can you please ask your question again?

BY MR. VAN HOVEN:

Q. Do you have an understanding as to whether that region of memory that includes the use counter value is read only?

A. So, it depends what you mean by read only, but at the very least, that region of memory

hypothetical because there are external questions that need to be resolved to answer it.

BY MR. VAN HOVEN:

Q. You do understand that my question is limited to the Atmel CryptoRF chip as implemented in Xi EndoWrist, correct?

A. I understand that much.

Q. Is the CryptoRF chip programmable once it's, I guess, out in the field in an Xi EndoWrist to your knowledge?

MS. CAHOY: Objection to form.

THE WITNESS: It depends what you mean by programmable.

BY MR. VAN HOVEN:

Q. Sure. Can values stored in memory of the CryptoRF chip be changed in the field when implemented in an Xi EndoWrist to your knowledge?

A. Sure. So, for instance, values can be decremented.

Q. Any other types of changes? Can other values be changed in an Atmel CryptoRF chip?

A. I don't know.

Q. Do you know if --

A. But hold on.

Q. Sure.

A. In the context of the EndoWrist Xi, I don't know. In the context of a CryptoRF chip in a vacuum, there are various things you can do to the chip as -- as specified in the datasheet.

Q. Including changing values that have previously been programmed into the chip; is that right?

MS. CAHOY: Objection to form.

THE WITNESS: Well, the chip has like a whole bunch of different features. It really depends on how the chip has been -- like what the actual design of your system is.

BY MR. VAN HOVEN:

Q. But one possibility with the CryptoRF chip is that you can change values that have previously been written -- written on to the chip, right?

MS. CAHOY: Objection to form.

BY MR. VAN HOVEN:

Q. That's something that's possible?

A. You would need to have a system set up to allow for that.

Q. Is the -- to your knowledge, is the use counter value that's stored on a CryptoRF chip in an Xi EndoWrist, is that value stored in -- in an encrypted form?

A. My understanding is that -- you said on an EndoWrist X/Xi. My understanding is that that value along with some other values are encrypted on that -- on those devices.

Q. What type of encryption is used for that?

(Whereupon, there was a pause for document examination.)

THE WITNESS: I don't think that's entirely clear from what I have seen.

BY MR. VAN HOVEN:

Q. So, you don't know what type of encryption is used for the use counter on the Xi

EndoWrist; is that right?

A. I think that's right. The evidence that I have seen has been conflicting on that front and in one case incorrectly referenced SHA as a type of encryption.

Q. But you don't personally know what type of encryption is used for the use counter on the Xi EndoWrist, right?

A. I don't believe I know all of the specifics of the cryptography used to encrypt the use counter and other information on the CryptoRF chips.

Q. What specifics do you know of the cryptography -- cryptography used to encrypt the use counter on the Xi EndoWrists?

A. I know the information in the datasheet about various things that are supported with respect to cryptography on these chips.

Q. But you don't know what Intuitive uses within that datasheet?

A. I don't know what they ultimately

selected.

Q. If you were tasked to attempt to circumvent the encryption of the use counter on the Xi EndoWrist, how would you go about that?

MS. CAHOY: Objection to form.

THE WITNESS: Oh, that's like a really complicated question. I don't think I could -- that's an entire like work engagement. That would take a lot of analysis just to figure out how to even approach the problem.

BY MR. VAN HOVEN:

Q. But let's just assume that you have access to the Atmel CryptoRF chip that has a use counter value on it that is encrypted, okay?

A. Okay.

Q. In that, you can either physically or wirelessly communicate with the chip?

A. Okay.

Q. And that you have the datasheet that tells you the types of encryption that's implemented, --

A. Um-hum.

Q. -- right? And you -- you have that datasheet, right?

A. Yes.

Q. So, given that information based on your 15 to 20 years of information security experience, as a general approach, how would you go about trying to circumvent the encryption on the use counter within an Atmel CryptoRF chip?

A. So, I -- I just haven't done that analysis.

Q. I understand. I'm -- but you're here to testify as an expert in the area of information security and I just want to understand the general approach you would take.

MS. CAHOY: Objection to form.

THE WITNESS: Right. So, the problem is it's a specific problem for a specific chip, and I would need to do a good amount of legwork to figure out what that approach would be. I haven't done that legwork, so I don't know what my approach

would be.

BY MR. VAN HOVEN:

Q. What type of legwork is typically involved in trying to attack that sort of problem?

A. I would need to spend some time thinking about it.

Q. So, time is one piece of -- one part of that legwork?

A. I don't think time is what I would call part of any legwork. Time is just a resource that you need to have to do anything.

In the absence of any time at all, everything would stand still, right? So, it's not clear what that means.

Q. I'm not talking about us getting close to the speed of light or anything here, but I'm just trying to understand, you said that there would be legwork. And I'm just trying to, what is -- what is the kind of legwork that -- that you're envisioning to attack the problem of circumventing the encryption as we've described on the Atmel

CryptoRF chip?

A. Sure. So, the -- the truth is that's -- that's complicated, and I haven't really thought about it.

Q. But you'd have to think about it a little bit, right?

A. Yes, I would have to think about that.

Q. You'd have to look at the datasheet?

A. Certainly, looking at the datasheet would be a part of any legwork.

Q. You would have to --

A. That would be true.

Q. Excuse me. You would have to perform some sort of direct electrical or in -- indirect communication channel probing of the chip probably?

MS. CAHOY: Objection to form.

THE WITNESS: At -- at some stage in the process, you would need to connect to the chip, but I haven't really thought about when or how that would occur. So, I don't have any more insight into that.

BY MR. VAN HOVEN:

Q. Do you think that the encryption employed by the CryptoRF chip is particularly complicated compared to the sort of encryption you typically have worked with?

A. I don't have an opinion on that.

Q. You don't know one way or the other?

A. I would need to investigate it more to figure it out.

Q. And you understand or do you have an understanding that, that the use counter value at some point is transmitted from the EndoWrist to the robot?

A. Yes.

Q. Do you know if that value is transmitted in that encrypted form or if it's decrypted before it's transmitted?

A. I understand the value to be encrypted when it's transmitted.

Q. What's the basis of that understanding?

A. My understanding is from the datasheet

counting data areas of the RFID tag are one-time programmable.

That means they can be -- not be modified once written. Though, of course, they could be decremented, which is an important point.

And so it reads to me that Intuitive documents state that the data is encrypted both at rest and in motion.

BY MR. VAN HOVEN:

Q. And your opinion in that regard is based solely on those documents, right?

MS. CAHOY: Objection to form.

THE WITNESS: I can also see that the datasheet supports those configurations.

BY MR. VAN HOVEN:

Q. As far as the encryption while the -- and here I'm talking specifically about the communications between the Xi EndoWrist and the Xi robot.

As far as the encryption while the data is at motion -- in motion, what would be your

approach to try -- if you were trying to circumvent that encryption?

A. Well, that's -- again, that's sort of the same problem as trying to reverse engineer or break the chip and -- as whole, right?

If I could circumvent that communication, then I would know how -- if I knew how to do that, I would know how to break the communication protocol, so it's the same issue. I don't -- I haven't performed that analysis. I don't know.

Q. But -- but that is your -- your primary area of expertise and study over the last 20 years, right?

A. Yes, I've done many of these. They always require a very thorough set of, you know, thoughts and research and legwork before you can really come up with an approach, and I haven't done that. I haven't done that part of what my normal practice would be.

Q. Yeah. So, if you were to approach a problem like this in your normal practice, what

sort of legwork would you need to perform?

A. Right. So, I would need to look at the individual issues at play, and I would need to look at the product and how it's designed. Let me just think about it and come up with an approach, and that would kind of let me determine what legwork I need to do to then -- so, I would need to think about what I would need to know. Then I would need to think about from what I needed to know, I would know that -- learn that information and figure out from that what I would do to attack.

So, it's a multi-step process, and I haven't performed even the first step yet is the problem.

Q. You just haven't examined that for the Xi EndoWrist, right?

A. That's right. Yeah, I haven't performed an analysis of what would be required to break the device.

I reviewed Mr. Humphrey's analysis. I saw that wouldn't work, but I haven't performed an

Q. And so in your role kind of as a manager at Harbor Labs, are you involved in like providing quotes or estimates to -- to customers who ask you to do something like that?

A. Sometimes. I don't typically do the medical quotes.

Q. Okay. When -- when you're involved in -- in quoting one of these security-based activities, what -- what type of process do you undergo typically?

A. So, when drafting a quote, you -- you usually are going to get a sense of how many components are in the system, the complexity, the amount of code. You're going to look at the programming languages that are used, how old the design is, possibly information about its architecture. You're going to get information about design docs and manuals, but not just external ones, internal ones, and especially requirements documents and other internal information.

You'll study that, which is already a decent amount of work, and then you'll write a quote. Usually, you'll create an MSA and a SOW.

So, you'll write into your SOW at least enough to recover that initial legwork plus the, you know, amount to cover what you think the product is.

To be honest, it's a pretty tricky business providing an accurate quote. It seems that we tend to underquote quite a lot in -- in our work.

Q. Sometimes you -- you kind of use more -- end up using more time and resources than you originally quoted?

A. Because it's so inexact, you don't know how hard it is to perform a particular task until you start working on it. Things might not work in exactly the way you anticipated, and that's why legwork is so important. The more legwork you do, the more accurate your quote will be.

MR. VAN HOVEN: Okay. Dr. Martin, I

Kenneth A. Gallo (*pro hac vice*)
Paul D. Brachman (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, NW
Washington, DC 20006-1047
Telephone: (202) 223-7300
Facsimile: (202) 204-7420
Email: kgallo@paulweiss.com
Email: pbrachman@paulweiss.com

William B. Michael (*pro hac vice*)
Crystal L. Parker (*pro hac vice*)
Daniel A. Crane (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
1285 Avenue of the Americas
New York, NY 10019-6064
Telephone: (212) 373-3000
Facsimile: (212) 757-3990
Email: wmichael@paulweiss.com
Email: cparker@paulweiss.com
Email: dcrane@paulweiss.com

Joshua Hill Jr. (SBN 250842)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
535 Mission Street, 24th Floor
San Francisco, CA 94105
Telephone: (628) 432-5100
Facsimile: (628) 232-3101
Email: jhill@paulweiss.com

Attorneys for Defendant Intuitive Surgical, Inc.

[Additional counsel listed on signature page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SURGICAL INSTRUMENT SERVICE COMPANY, INC.,

Plaintiff,

v.

INTUITIVE SURGICAL, INC.,

Defendant.

Case No. 3:21-cv-03496-AMO

DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION IN LIMINE #4

Date: November 25, 2024
Time: 11:00 a.m.
Courtroom: 10

The Honorable Araceli Martínez-Olguín

PRELIMINARY STATEMENT

In an attempt to obtain overbroad, premature rulings limiting Intuitive's ability to offer testimony regarding technical aspects of its X/Xi EndoWrist products, Plaintiff SIS's Motion *in Limine* No. 4 seeks to limit the introduction of testimony, exhibits, and argument from both Intuitive expert Dr. Paul Martin and from unspecified Intuitive fact witnesses regarding reverse engineering X/Xi EndoWrists. Both prongs of SIS's motion should be denied.

First, SIS moves to limit Dr. Paul Martin's testimony at trial. Specifically, SIS asks this Court to preclude Dr. Martin from testifying "about reverse engineering the technology necessary to reset X/Xi EndoWrists, including whether or not SIS could have broken the encryption on X/Xi EndoWrists," arguing such testimony is outside the scope of his expert report. Mot. at 1–2. Intuitive has no intention of eliciting from Dr. Martin testimony that is beyond the scope of his report, and already, and to avoid burdening the Court with an unnecessary motion, offered to stipulate that no such testimony will be offered from Dr. Martin. Ex. 1 ¶ 1. But SIS refused to agree to Intuitive's proposed stipulation. Ex. 2. As to Dr. Martin, Intuitive respectfully submits that the Court should either deny SIS's motion in its entirety or order the relief to which Intuitive already offered to stipulate and deny the motion as moot.

Second, as to lay witness testimony, to the extent SIS is asking the Court to preclude Intuitive from introducing argument or testimony from unidentified fact witnesses about "reverse engineer[ing] the X/Xi EndoWrist encryption," Mot. at 5, the Court should reject SIS's request as both contrary to law and premature. Consistent with Federal Rules of Evidence 602 and 701, Intuitive's lay witnesses will offer testimony at trial based on their personal knowledge and experiences at Intuitive. Such testimony is not transformed into "undisclosed expert testimony," *id.* at 6, simply because the underlying facts and data are technical in nature. Indeed, courts in this district routinely allow lay witnesses to testify about their opinions when those opinions are based on the witness's personal knowledge—including particularized knowledge and experience relating to a witness's employment. And, because SIS has not actually identified the "opinion testimony and argument" it seeks to exclude, its request should also be denied as premature.

ARGUMENT

I. SIS'S MOTION *IN LIMINE* 4 IS MOOT AS TO DR. PAUL MARTIN

Consistent with its obligations under Rule 26(a)(2)(B), Intuitive has no intention of eliciting testimony from Dr. Martin at trial that is beyond the scope of the opinions offered in his expert report. Intuitive informed SIS of its position on November 1, 2024, when it proposed that the parties agree and stipulate that:

> Intuitive will not seek to introduce testimony from Dr. Martin at trial beyond the scope of the opinions offered by Dr. Martin in his expert report. In particular, Intuitive Surgical will not seek to offer testimony from Dr. Martin regarding the steps or processes required to reverse engineer X/Xi EndoWrists including whether or not SIS could have broken the encryption of X/Xi EndoWrists.

Ex. 1 ¶ 1; Ex. 3. Yet, SIS has refused to withdraw its Motion as to Dr. Martin. To the extent that SIS is seeking some relief beyond the relief to which Intuitive offered to stipulate, there is no basis for it and SIS's motion should be denied.

To be sure, and as Intuitive has communicated to SIS, Intuitive will question Dr. Martin at trial about the opinions and bases therefor that are disclosed in his expert report, including but not limited to his opinions regarding (i) the background of cybersecurity and cryptography, (ii) the security vulnerabilities of wireless systems and the use of encryption as a mitigation measure, (iii) the assessment, use, and encryption of the Atmel RFID chip in the X/Xi EndoWrists, and (iv) the benefits and improvements of the Atmel RFID chip over the wired chip used in the S/Si EndoWrists. Ex. 1 ¶ 2. Additionally, Intuitive may cross examine SIS's witnesses—expert and otherwise—regarding reverse engineering of X/Xi EndoWrists, including whether or not SIS could have broken the encryption of X/Xi EndoWrists.[1] *Id.* But no such examination supports SIS's request to exclude here.

[1] For example, SIS has disclosed that it may call Stan Hamilton to testify about the "ability to reset the EndoWrist Xi usage counter," Kevin May to testify about "reverse engineering the Xi," and Clif Parker to testify about "efforts to reset usage counter and repair X/Xi EndoWrists." Dkt. 278-3, App. E at 5–6. And SIS will call Kurt Humphrey to "testify to matters disclosed in his expert reports." *Id.* at 3. As SIS itself notes in its Motion, such matters include reverse engineering of the X and Xi EndoWrist encryption. Mot. at 1–2.

Moreover, even if Intuitive intended to elicit testimony beyond the scope of Dr. Martin's report, which it does not, SIS's motion should still be denied because it is unspecified, over broad, and premature. It is well-accepted that expert testimony must be limited to the contents of the expert's report, but issues regarding the scope of testimony are best "addressed during trial as particular questions of admissibility arise." *Hudson* v. *Alaska Airlines, Inc.*, 2019 U.S. Dist. LEXIS 153418 at *7 (N.D. Cal. Sep. 9, 2019) (denying plaintiff's motion "to preclude defendant from introducing expert testimony not disclosed in its expert disclosures" where the plaintiff had "not specified any particular evidence she [sought] to exclude, but rather refer[ed] to unbounded, broad categories of evidence"); *Fernandez* v. *Taser Int'l, Inc.*, 2008 WL 4775779, at *3 (N.D. Cal. Oct. 27, 2008) (denying as premature multiple motions *in limine* seeking to exclude or include hypothetical evidence, including hypothetical expert testimony).

Because Intuitive does not intend to elicit testimony from Dr. Martin beyond the scope of his report, including testimony regarding the feasibility or efforts required to reverse engineer X/Xi EndoWrists or SIS's ability to do so, SIS's Motion should be denied as to Dr. Martin's opinions.

II. SIS'S REQUEST TO EXCLUDE UNSPECIFIED LAY "OPINION TESTIMONY AND ARGUMENT" SHOULD BE DENIED BECAUSE IT IS UNSUPPORTED BY LAW AND PREMATURE.

Without pointing to a single specific lay witness, let alone to proposed testimony from Intuitive for any such witness, SIS asks the Court to exclude any argument or "lay opinion testimony about the feasibility, timing, resources needed, and effort required to reverse engineer the X/Xi EndoWrist encryption and reset the usage counter." Mot. at 5. SIS claims that such (as of yet unidentified) evidence would fail to comply with Fed. R. Evid. 701. SIS's position seems to be that any testimony "about reverse engineering the X/Xi EndoWrist encryption in order to reset the usage counter" must "be based on scientific, technical, or other specialized knowledge," and so it would be improper for an Intuitive employee to testify about these topics without having been disclosed as an expert. *Id.* at 5–6. SIS's request is wholly inconsistent with how courts in this District address the scope of lay witness testimony. Moreover, its request to exclude unspecified testimony and argument is both hypothetical and premature. As a result, it should be denied.

Intuitive is in the business of designing and making the complex surgical systems that are the subject of this lawsuit. Given Intuitive's business, it should come as no surprise to SIS that various Intuitive employees who will testify at trial have personal knowledge and experience related to the design, development, and testing of the Intuitive products and technology they work with on a day-to-day basis. Indeed, SIS deposed numerous Intuitive employees, including several engineers, on their technical knowledge and experience as it related to Intuitive's products.

The knowledge, experience, and opinions Intuitive's lay witnesses hold as a result of their day-to-day work at Intuitive is permissible trial testimony and, contrary to any suggestion by SIS, need not have been disclosed under Rule 26(a)(2)(B) simply because some of that knowledge is technical in nature. That is because, consistent with Rule 701, courts in this District routinely "allow lay opinion testimony based upon particularized knowledge obtained by virtue of the witness's position in the business." *In re Google AdWords Litig.*, 2012 WL 28068, at *4 (N.D. Cal. Jan. 5, 2012), *rev'd and remanded sub nom. Pulaski & Middleman, LLC* v. *Google, Inc.*, 802 F.3d 979 (9th Cir. 2015). None of SIS's cases say otherwise—nor could they—because "the rules of evidence 'have long permitted a person to testify to opinions about their own business based on their personal knowledge of their business.'" *Id.* (citation omitted). That a particular witness's position in the business involves scientific or other technical knowledge does not alter the rules of evidence. *Id.*; *United States* v. *Brody*, 2023 WL 2541118, at *3 (N.D. Cal. Mar. 16, 2023) (same); *see also USA* v. *Chen*, 2021 WL 2662116, at *9 (N.D. Cal. June 29, 2021) (denying motion *in limine* seeking to exclude lay witness opinion testimony and explaining that "such opinion testimony is admitted 'not because of experience, training or specialized knowledge within the realm of an expert, but because of the particularized knowledge that the witness has by virtue of his or her position in the business'") (quoting Fed. R. Evid. 701 advisory committee's note to 2000 amendment).

The court's application of the above principle in *Google AdWords* is instructive. There, the court found that Google's Chief Economist was qualified to explain, as a lay witness, how the at-issue technology worked, how it behaved, and how it responded under variable scenarios, and held that the Chief Economist could "offer lay witness opinions regarding Google's business, so

long as those opinions are based on his own personal, particularized knowledge and experience relating to his employment at Google." *In re Google AdWords Litig.*, 2012 WL 28068, at *5. As the court explained, "just because the underlying facts and data are technical in nature does not transform the information into 'expert testimony' when those facts are within the personal knowledge and experience of the company's employee." *Id.* Likewise, the court allowed a senior Google employee to offer testimony based on facts and data analysis within the scope of his employment, including data that the witness reviewed after plaintiffs had filed their lawsuit, and allowed a Google manager to offer lay witness opinions "so long as those opinions [were] based on his own personal, particularized knowledge and experience relating to his employment at Google." *Id.* at *7. Because any testimony elicited from Intuitive's lay witnesses will be based on their knowledge and experience related to their employment, SIS's attempt to characterize such testimony as improper expert testimony—opinion or otherwise—that should have been disclosed pursuant to Rule 26(a)(2)(B) should be rejected. *Id.* at *5 (rejecting request to strike lay witness's opinion testimony "as expert testimony in violation of Rule 26 disclosures" where the opinion testimony regarded Google's business, including its AdWords business—the subject matter of the litigation).

The cases cited by SIS (Mot. at 5) are readily distinguishable from the facts here, and none of those cases supports SIS's request. For example, in *Sapiano* v. *Millennium Entertainment,* 2013 WL 12122467, * 4 (C.D. Cal. Nov. 20, 2013), the court disallowed lay opinion testimony that was based solely on an expert report and expert testimony that the court had excluded for other reasons. In *Haro* v. *GGP-Tucson Mall LLC,* 2019 WL 369269, * 3–4 (D. Ariz. Jan. 30, 2019), the court precluded physician testimony on causation where the plaintiff first visited the physicians months after a fall and the physicians could not present information of plaintiff's condition prior to the fall, reasoning that such a causation opinion necessarily would be based on the physicians' specialized medical training. Finally, in *Malkin* v. *Federal Insurance Company*, 2023 WL 6967458, *15–16 (C.D. Cal. Oct. 20, 2023), the court precluded lay witness testimony on causation of alleged sediment settlement damage to the plaintiff's home, limiting lay witness testimony to their personal observations. None of these cases suggest that lay opinion testimony based on a

witness's day-to-day personal knowledge and experience at work, about that work, is improper under Rule 701.

Moreover, SIS's request should be denied for the independent reason that it is unspecific, hypothetical, and premature. SIS does not even attempt to identify a single Intuitive lay witness who it believes will offer improper testimony. Like SIS, the defendant in *Brody* moved to exclude lay testimony offered as expert witness testimony but pointed to "no specific testimony or witness" and provided "no indication that the government plan[ned] on introducing such testimony." *Brody*, 2023 WL 2541118, at *3. Surmising that the motion may be directed at employees who would "testify about technical topics within their personal knowledge and experience," the court denied the motion,[2] noting that the defendant could raise an objection "if the issue c[ame] up in a more specific context at trial." *Id.* at *4; *see Fernandez*, 2008 WL 4775779, at *3 (denying as premature multiple motions *in limine* seeking to exclude or include hypothetical evidence). The same result is appropriate here.

CONCLUSION

For these reasons, Intuitive respectfully requests that the Court deny SIS's Motion *in Limine* No. 4.

[2] "Witnesses may testify to matters for which they have personal knowledge. Fed. R. Evid. 602. And lay witnesses may testify to their opinions under FRE 701, outside of the scope of expert testimony permitted by FRE 702." *Id.* at *3.

Dated: November 7, 2024

By: /s/ *Kenneth A. Gallo*
Kenneth A. Gallo

Kenneth A. Gallo (*pro hac vice*)
Paul D. Brachman (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, NW
Washington, DC 20006-1047
Telephone: (202) 223-7300
Facsimile: (202) 204-7420
Email: kgallo@paulweiss.com
Email: pbrachman@paulweiss.com

William B. Michael (*pro hac vice*)
Crystal L. Parker (*pro hac vice*)
Daniel A. Crane (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
1285 Avenue of the Americas
New York, NY 10019-6064
Telephone: (212) 373-3000
Facsimile: (212) 757-3990
Email: wmichael@paulweiss.com
Email: cparker@paulweiss.com
Email: dcrane@paulweiss.com

Joshua Hill Jr. (SBN 250842)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
535 Mission Street, 24th Floor
San Francisco, CA 94105
Telephone: (628) 432-5100
Facsimile: (628) 232-3101
Email: jhill@paulweiss.com

Sonya D. Winner (SBN 200348)
COVINGTON & BURLINGTON LLP
415 Mission Street, Suite 5400
San Francisco, California 94105-2533
Telephone: (415) 591-6000
Facsimile: (415) 591-6091
Email: swinner@cov.com

Kathryn E. Cahoy (SBN 298777)
COVINGTON & BURLINGTON LLP
3000 El Camino Real

5 Palo Alto Square, 10th Floor
Palo Alto, California 94306-2112
Telephone: (650) 632-4700
Facsimile: (650) 632-4800
Email: kcahoy@cov.com

Andrew Lazerow (*pro hac vice*)
COVINGTON & BURLINGTON LLP
One City Center 850 Tenth Street NW
Washington DC 20001-4956
Telephone: (202) 662-6000
Facsimile: (202) 662-6291
Email: alazerow@cov.com

Allen Ruby (SBN 47109)
ALLEN RUBY, ATTORNEY AT LAW
15559 Union Ave. #138
Los Gatos, California 95032
Telephone: (408) 477-9690
Email: allen@allenruby.com

Attorneys for *Defendant Intuitive Surgical, Inc.*

CERTIFICATE OF SERVICE

On November 7, 2024, I caused a copy of Intuitive's Opposition to SIS's Motion *in Limine* No. 4 to be electronically served via email on counsel of record for Surgical Instrument Service Company, Inc.

Dated: November 7, 2024

By: */s/ Kenneth A. Gallo*
Kenneth A. Gallo

Kenneth A. Gallo (*pro hac vice*)
Paul D. Brachman (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, NW
Washington, DC 20006-1047
Telephone: (202) 223-7300
Facsimile: (202) 204-7420
Email: kgallo@paulweiss.com
Email: pbrachman@paulweiss.com

William B. Michael (*pro hac vice*)
Crystal L. Parker (*pro hac vice*)
Daniel A. Crane (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
1285 Avenue of the Americas
New York, NY 10019-6064
Telephone: (212) 373-3000
Facsimile: (212) 757-3990
Email: wmichael@paulweiss.com
Email: cparker@paulweiss.com
Email: dcrane@paulweiss.com

Joshua Hill Jr. (SBN 250842)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
535 Mission Street, 24th Floor
San Francisco, CA 94105
Telephone: (628) 432-5100
Facsimile: (628) 232-3101
Email: jhill@paulweiss.com

Attorneys for Defendant Intuitive Surgical, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SURGICAL INSTRUMENT SERVICE COMPANY, INC.,
Plaintiff,
v.
INTUITIVE SURGICAL, INC.,
Defendant.

Case No. 3:21-cv-03496-AMO

DECLARATION OF CRYSTAL L. PARKER IN SUPPORT OF DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION *IN LIMINE* #4

The Honorable Araceli Martínez-Olguín

I, CRYSTAL PARKER, declare as follows:

1. I am an attorney licensed to practice in New York and Massachusetts and am admitted *pro hac vice* to practice before this Court. I am a partner with the law firm of Paul, Weiss, Rifkind, Wharton & Garrison LLP ("Paul, Weiss"), counsel for Intuitive Surgical, Inc. ("Intuitive" or "Defendant") in this matter. I have personal knowledge of the facts set forth herein, and if called to testify, I could and would testify competently hereto.

2. Attached to this declaration as **Exhibit 1** is a true and correct copy of the stipulation Intuitive proposed to Surgical Instrument Service Company's ("SIS" or "Plaintiff") on November 1, 2024 to resolve SIS's Motion *In Limine* No. 4.

3. Attached to this declaration as **Exhibit 2** is a true and correct copy of an email from Paul D. Brachman, counsel for Intuitive, to Josh Van Hoven, counsel for SIS, and others, attaching **Exhibit 1**, dated November 1, 2024.

4. Attached to this declaration as **Exhibit 3** is a true and correct copy of an email from Mr. Van Hoven to Mr. Brachman and others, dated November 4, 2024.

I declare under the penalty of perjury under the laws of the United States that the foregoing is true and correct.

Dated: November 7, 2024

By: /s/ *Crystal L. Parker*.

CRYSTAL L. PARKER

EXHIBIT 1

to

CRYSTAL L. PARKER DECLARATION IN SUPPORT OF DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION IN LIMINE #4

Kenneth A. Gallo (*pro hac vice*)
Paul D. Brachman (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, NW
Washington, DC 20006-1047
Telephone: (202) 223-7300
Facsimile: (202) 204-7420
Email: kgallo@paulweiss.com
Email: pbrachman@paulweiss.com

William B. Michael (*pro hac vice*)
Crystal L. Parker (*pro hac vice*)
Daniel A. Crane (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
1285 Avenue of the Americas
New York, NY 10019-6064
Telephone: (212) 373-3000
Facsimile: (212) 757-3990
Email: wmichael@paulweiss.com
Email: cparker@paulweiss.com
Email: dcrane@paulweiss.com

Joshua Hill Jr. (SBN 250842)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
535 Mission Street, 24th Floor
San Francisco, CA 94105
Telephone: (628) 432-5100
Facsimile: (628) 232-3101
Email: jhill@paulweiss.com

Attorneys for Defendant Intuitive Surgical, Inc.

[Additional counsel listed on signature page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SURGICAL INSTRUMENT SERVICE COMPANY, INC.,
Plaintiff,
v.
INTUITIVE SURGICAL, INC.,
Defendant.

Case No. 3:21-cv-03496-AMO

STIPULATIONS REGARDING THE TESTIMONY OF DR. PAUL D. MARTIN

The Honorable Araceli Martínez-Olguín

Plaintiff Surgical Instrument Service Company, Inc. ("SIS"), and Defendant Intuitive Surgical, Inc. ("Intuitive") stipulate to the following regarding the trial testimony of Defendant Intuitive's Expert Dr. Paul D. Martin:

1. The Parties agree that, consistent with Rule 26(a)(2)(B), Intuitive will not seek to introduce testimony from Dr. Martin at trial beyond the scope of the opinions offered by Dr. Martin in his expert report. In particular, Intuitive Surgical will not seek to offer testimony from Dr. Martin regarding the steps or processes required to reverse engineer X/Xi EndoWrists including whether or not SIS could have broken the encryption of X/Xi EndoWrists.

2. Nothing in this Stipulation shall prevent Intuitive from presenting testimony from Dr. Martin regarding the opinions and bases therefore disclosed in his expert report including but not limited to his opinions regarding the background of cybersecurity and cryptography, security vulnerabilities of wireless systems and the use of encryption as a mitigation measure, the assessment, use, and encryption of the Atmel RFID chip in the X/Xi EndoWrists, and the benefits and improvements of the Atmel RFID chip over the wired chip used in the S/Si EndoWrists. In addition, nothing in this Stipulation shall prevent Intuitive from cross examining witnesses regarding reverse engineering of X/Xi EndoWrists including whether or not SIS could have broken the encryption of X/Xi EndoWrists.

IT IS SO STIPULATED, THROUGH COUNSEL OF RECORD.

Dated: November , 2024

By: *DRAFT*
Kenneth A. Gallo

Kenneth A. Gallo (*pro hac vice*)
Paul D. Brachman (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, NW
Washington, DC 20006-1047
Telephone: (202) 223-7300
Facsimile: (202) 204-7420
Email: kgallo@paulweiss.com
Email: pbrachman@paulweiss.com

William B. Michael (*pro hac vice*)
Crystal L. Parker (*pro hac vice*)
Daniel A. Crane (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
1285 Avenue of the Americas
New York, NY 10019-6064
Telephone: (212) 373-3000
Facsimile: (212) 757-3990
Email: wmichael@paulweiss.com
Email: cparker@paulweiss.com
Email: dcrane@paulweiss.com

Joshua Hill Jr. (SBN 250842)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
535 Mission Street, 24th Floor
San Francisco, CA 94105
Telephone: (628) 432-5100
Facsimile: (628) 232-3101
Email: jhill@paulweiss.com

Sonya D. Winner (SBN 200348)
COVINGTON & BURLINGTON LLP
415 Mission Street, Suite 5400
San Francisco, California 94105-2533
Telephone: (415) 591-6000
Facsimile: (415) 591-6091
Email: swinner@cov.com

Kathryn E. Cahoy (SBN 298777)
COVINGTON & BURLINGTON LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, California 94306-2112
Telephone: (650) 632-4700
Facsimile: (650) 632-4800
Email: kcahoy@cov.com

Andrew Lazerow (*pro hac vice*)
COVINGTON & BURLINGTON LLP
One City Center 850 Tenth Street NW
Washington DC 20001-4956
Telephone: (202) 662-6000
Facsimile: (202) 662-6291
Email: alazerow@cov.com

Allen Ruby (SBN 47109)
ALLEN RUBY, ATTORNEY AT LAW
15559 Union Ave. #138
Los Gatos, California 95032
Telephone: (408) 477-9690
Email: allen@allenruby.com

Attorneys for *Defendant Intuitive Surgical, Inc.*

Dated: November , 2024

By: *DRAFT*
Joshua V. Van Hoven

Joshua V. Van Hoven (CSB No. 262815)
MCCAULLEY LAW GROUP LLC
Email: josh@mccaulleylawgroup.com
3001 Bishop Dr., Suite 300
San Ramon, California 94583
Telephone: (925) 302-5941

Richard T. McCaulley (*pro hac vice*)
MCCAULLEY LAW GROUP LLC
Email: richard@mccaulleylawgroup.com
180 N. Wabash Avenue, Suite 601
Chicago, Illinois 60601
Telephone: (312) 330-8105

Attorneys for Plaintiff *Surgical Instrument Service Company, Inc.*

E-Filing Attestation

I, Kenneth A. Gallo, am the ECF User whose ID and password are being used to file this document. In compliance with Civil Local Rule 5-1(i)(3), I hereby attest that each of the signatories identified above have concurred in this filing.

DRAFT

EXHIBIT 2

to

CRYSTAL L. PARKER DECLARATION IN SUPPORT OF DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION IN LIMINE #4

From: Brachman, Paul D
Sent: Friday, November 1, 2024 03:33 PM
To: Josh Van Hoven; Gallo, Kenneth A; Michael, William; Hill, Joshua; Parker, Crystal; Milligan, Heather C; allen@allenruby.com; Cahoy, Kathryn; Lazerow, Andrew; Winner, Sonya
Cc: Richard McCaulley; Steve Sherry
Subject: RE: SIS MIL 2
Attachments: DRAFT MIL 2 Stipulation (11-01-24)(20314910.6).docx; DRAFT MIL 3 Stipulation (11-01-24)(20327915.2).docx; DRAFT MIL 4 Stipulation (11-01-24)(20314938.2).docx

Josh,

We would be prepared to enter into the attached stipulations to resolve your MILs 2-4. Please let us know by Monday, November 4, if SIS is willing to so stipulate, and thereby resolve the motions without the need for Court intervention.

Best,
Paul

Paul Brachman | Partner
Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW | Washington, DC 20006-1047
+1 202 223 7440 (Direct Phone) | +1 202 379 4098 (Direct Fax)
pbrachman@paulweiss.com | www.paulweiss.com

From: Josh Van Hoven <josh@mccaulleylawgroup.com>
Sent: Monday, October 28, 2024 11:05 PM
To: Josh Van Hoven <josh@mccaulleylawgroup.com>; Gallo, Kenneth A <kgallo@paulweiss.com>; Michael, William <wmichael@paulweiss.com>; Hill, Joshua <jhill@paulweiss.com>; Parker, Crystal <cparker@paulweiss.com>; Brachman, Paul D <pbrachman@paulweiss.com>; Milligan, Heather C <hmilligan@paulweiss.com>; allen@allenruby.com; Cahoy, Kathryn <kcahoy@cov.com>; Lazerow, Andrew <alazerow@cov.com>; Winner, Sonya <swinner@cov.com>
Cc: Richard McCaulley <richard@mccaulleylawgroup.com>; Steve Sherry <steve@mccaulleylawgroup.com>
Subject: SIS MIL 2

Counsel,
See attached for service SIS's Motion in Limine #2.
Best,
- Josh

Joshua Van Hoven
(925) 302-5941
3001 Bishop Dr., Suite 300
San Ramon, CA 94583
josh@mccaulleylawgroup.com

EXHIBIT 3

to

CRYSTAL L. PARKER DECLARATION IN SUPPORT OF DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION IN LIMINE #4

From: Josh Van Hoven <josh@mccaulleylawgroup.com>
Sent: Monday, November 4, 2024 12:14 PM
To: Brachman, Paul D; Gallo, Kenneth A; Michael, William; Hill, Joshua; Parker, Crystal; Milligan, Heather C; allen@allenruby.com; Cahoy, Kathryn; Lazerow, Andrew; Winner, Sonya
Cc: Richard McCaulley; Steve Sherry
Subject: RE: SIS MIL 2

Paul,

We agree to the stipulations re MILs 2 and 3 if they are presented such as by administrative motions that include (respectively) the original motions, the previously attached stipulations, and proposed orders with language of the stipulations to be entered by the Court.

We do not agree to the stipulation on MIL 4.

Best,
- Josh

Joshua Van Hoven
(925) 302-5941
josh@mccaulleylawgroup.com

From: Brachman, Paul D <pbrachman@paulweiss.com>
Sent: Friday, November 1, 2024 12:33 PM
To: Josh Van Hoven <josh@mccaulleylawgroup.com>; Gallo, Kenneth A <kgallo@paulweiss.com>; Michael, William <wmichael@paulweiss.com>; Hill, Joshua <jhill@paulweiss.com>; Parker, Crystal <cparker@paulweiss.com>; Milligan, Heather C <hmilligan@paulweiss.com>; allen@allenruby.com; Cahoy, Kathryn <kcahoy@cov.com>; Lazerow, Andrew <alazerow@cov.com>; Winner, Sonya <swinner@cov.com>
Cc: Richard McCaulley <richard@mccaulleylawgroup.com>; Steve Sherry <steve@mccaulleylawgroup.com>
Subject: RE: SIS MIL 2

Josh,

We would be prepared to enter into the attached stipulations to resolve your MILs 2-4. Please let us know by Monday, November 4, if SIS is willing to so stipulate, and thereby resolve the motions without the need for Court intervention.

Best,
Paul

Paul Brachman | Partner
Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW | Washington, DC 20006-1047
+1 202 223 7440 (Direct Phone) | +1 202 379 4098 (Direct Fax)
pbrachman@paulweiss.com | www.paulweiss.com

From: Josh Van Hoven <josh@mccaulleylawgroup.com>
Sent: Monday, October 28, 2024 11:05 PM
To: Josh Van Hoven <josh@mccaulleylawgroup.com>; Gallo, Kenneth A <kgallo@paulweiss.com>; Michael, William <wmichael@paulweiss.com>; Hill, Joshua <jhill@paulweiss.com>; Parker, Crystal <cparker@paulweiss.com>; Brachman, Paul D <pbrachman@paulweiss.com>; Milligan, Heather C <hmilligan@paulweiss.com>; allen@allenruby.com; Cahoy, Kathryn <kcahoy@cov.com>; Lazerow, Andrew <alazerow@cov.com>; Winner, Sonya <swinner@cov.com>
Cc: Richard McCaulley <richard@mccaulleylawgroup.com>; Steve Sherry <steve@mccaulleylawgroup.com>
Subject: SIS MIL 2

Counsel,
See attached for service SIS's Motion in Limine #2.
Best,
- Josh

Joshua Van Hoven
(925) 302-5941
3001 Bishop Dr., Suite 300
San Ramon, CA 94583
josh@mccaulleylawgroup.com

FILER'S ATTESTATION

I, Joshua Van Hoven, am the ECF User whose ID and password are being used to file this document. In compliance with Civil Local Rule 5-1(i)(3), I hereby attest that the signatories identified above have concurred in this filing.

Dated: November 11, 2024

McCAULLEY LAW GROUP LLC
By: */s/ Joshua Van Hoven*
JOSHUA V. VAN HOVEN (CSB#262815)
E-Mail: josh@mccaulleylawgroup.com
3001 Bishop Dr., Suite 300
San Ramon, California 94583
Telephone: 925.302.5941

Attorney for SURGICAL INSTRUMENT SERVICE COMPANY, INC.